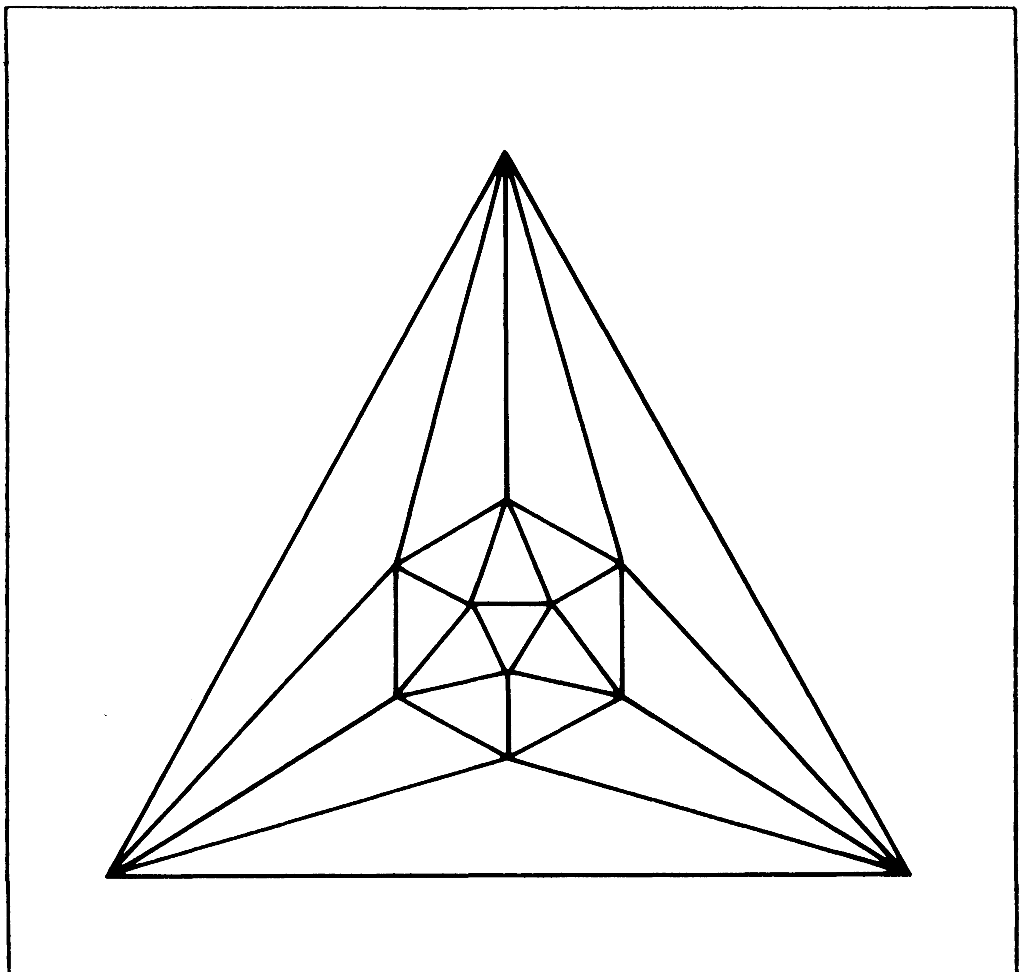
Vol. 61 No. 4 October 1988

MATHEMATICS MAGAZINE



- Kepler's Spheres and Rubik's Cube
- Catalan Strikes Again!
- The Centrality of Mathematics

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. 54, pp. 44–45, 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: G. L. Alexanderson, Editor, Mathematics Magazine, Santa Clara University, Santa Clara, CA 95053. 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 one copy and keep one copy. Illustrations should be carefully prepared on separate sheets in black ink, the original without lettering and two copies with lettering added.

AUTHORS

Richard K. Guy, doctoral supervisor of his present coauthor, sometime Governor-at-Large of the MAA, currently on the Council of the A.M.S., coauthor of *Winning Ways for your Mathematical Plays*, editor of *Reviews in Number Theory, 1973–83*, and of the Unsolved Problems section of the *Monthly*, believes in climbing mountains and in getting as much mathematics to as many people as possible. The Catalan numbers are one of several good ways of doing that.

Roger Eggleton has B.Sc. (Hons) and M.A. degrees from the University of Melbourne, and a Ph.D. from the University of Calgary. His doctorate was gained in 1973, culminating three pleasant and pun-filled years under the supervision of Richard Guy. When he spent four months of his last sabbatical leave in Calgary he stayed with the Guys and, naturally, Richard and he discussed many mathematical problems. They are both problem-solvers from "way back," and both are keenly interested in combinatorics, so it was natural for them to get intrigued with the problem which led to this joint paper. Incidentally, Roger will be Professor of Mathematics at the University of Brunei Darussalam from the start of 1989.

Judith V. Grabiner, who benefited from the history, philosophy, and literature of the storied Chicago General Education program while getting her bachelor's degree in mathematics from the University of Chicago, received her Ph.D. in the History of Science from Harvard in 1966. In teaching the history of mathematics, and mathematics for nonmajors, she has developed the approach reflected in this article. She has edited the Book Review department of *Historia Mathematica*, chaired the Southern California section of the Mathematical Association of America, and written *The Origins of Cauchy's Rigorous Calculus* (MIT, 1981). Dr. Grabiner is now Professor of Mathematics at Pitzer College in Claremont, California.

Acknowledgements: The filler on p. 230 was kindly provided by Ralph P. Boas. We are grateful for the permission to reprint the article by Judith Grabiner from the Proceedings of the International Congress of Mathematicians, 1986.

Vol. 61 No. 4 October 1988

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 $11 included as part of the annual dues. (Annual dues for regular members, exclusive of annual subscription prices for MAA journals, are $22. Student, unemployed and emeritus members receive a 50% discount; new members receive a 30% dues discount for the first two years of membership.) The nonmember/library subscription price is $28 per year. Bulk subscriptions (5 or more copies) are available to colleges and universities for classroom distribution to undergraduate students at a 41% discount ($6.50 per copy—minimum order $32.50).

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. 20077-9564.

PRINTED IN THE UNITED STATES OF AMERICA

ARTICLES

Catalan Strikes Again! How Likely Is a Function to Be Convex?

ROGER B. EGGLETON
The University of Newcastle,
Newcastle, N.S.W., 2308, Australia

RICHARD K. GUY
The University of Calgary
Calgary, Alberta, Canada, T2N 1N4

How to write a paper? An intriguing title is a good start. But what then? If we polish it until it shines, and it manages to get past editor and referee, will it show the sweat and pain that went into both the evolution of the content and the smoothing of the exposition? But the evolution may be pedagogically the most important part. Can we spare the time and space to explore blind alleys, to display methods which failed to work, to do calculations later found to be redundant, to exhibit manipulations which were eventually eliminated?

The Catalan numbers,

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, \ldots$$

are truly ubiquitous, but are not nearly as well known as the Fibonacci numbers, for example. They don't appear in many combinatorial texts, but you can find them in Comtet [**2**] and Roberts [**9**]. They appeared in Martin Gardner's column [**5**] and in Chapter 3 of Neil Sloane's *Handbook* [**10**]. Will Brown's article [**1**] has a bibliography of 46 items, and Henry Gould's collection [**7**] has more than ten times as many! The earliest references (Segner, Euler, Kotelnikow) date from more than half a century before Catalan was born. They have been the subject of several theses: for example, Mike Kuchinski [**8**] explores the correspondences between their many manifestations. Some of the better known are:

1. The number of ways of parenthesizing a (non-associative) product of $n+1$ factors.
2. The quotient when the middle binomial coefficient, $\binom{2n}{n}$, is divided by $n+1$.
3. The number of ways of chopping an (irregular) $(n+2)$-gon into n triangles by $n-1$ non-intersecting diagonals.
4. The self-convolving sequence, $c_0 = 1$,

$$c_{n+1} = c_0c_n + c_1c_{n-1} + c_2c_{n-2} + \cdots + c_nc_0 \qquad (n \geqslant 0).$$

5. The number of (plane) binary trees with n internal (trivalent) nodes.
6. The number of plane rooted trees with n edges.
7. The coefficients in the power series expansion of the generating function $(1-\sqrt{1-4x})/2x$.

8. The number of mountain ranges you can draw, using n upstrokes and n downstrokes.

9. The number of single mountains (cols between peaks are no longer allowed to be as low as sea level) you can draw with $n+1$ upstrokes and $n+1$ downstrokes.

10. The number of paths from $(0,0)$ to (n,n) (resp. $(n+1,n+1)$) increasing just one coordinate by one at each step, without crossing (resp. meeting) the diagonal $x=y$ at any point between (a thin disguise of 8 and 9).

11. Another disguise is the number of ways n votes can come in for each of two candidates A and B in an election, with A never behind B.

12. The recurring sequence $c_0=1$, $(n+2)c_{n+1}=(4n+2)c_n$ $(n\geqslant 0)$.

13. The number of different frieze patterns [3] with $n+1$ rows.

14. The number of ways $2n$ people, seated round a table, can shake hands in n pairs, without their arms crossing.

15. The number of Murasaki diagrams [7], [8] of n colored incense sticks which do not involve crossings.

Here's another:

J. van de Lune asked for the probability that the function

$$(0,f_0),(1,f_1),(2,f_2),\ldots,(n,f_n)$$

should be convex, if the $n+1$ values of f_k are randomly chosen from the interval $[0,1]$.

What is a convex function? In the literature you can find two meanings, depending on whether you're looking at it from above or below! Here it doesn't matter which, since you can turn the problem upside-down. We mean that the slope is increasing: the definition can be stated so that it covers both the continuous case, and the discrete one that we have here. A function is **convex** provided any three of its values $f_i, f_j, f_k (i<j<k)$ satisfy the inequality

$$\frac{f_i-f_j}{i-j}\leqslant\frac{f_j-f_k}{j-k}.$$

Geometrically, the graph between two points doesn't come above the chord joining them. In the discrete case, with values at equally spaced points, it suffices to look at consecutive values, and say that no value exceeds the mean of its neighbors.

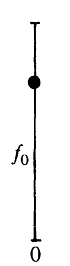


FIGURE 0
$n=0$.

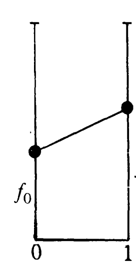


FIGURE 1
$n=1$.

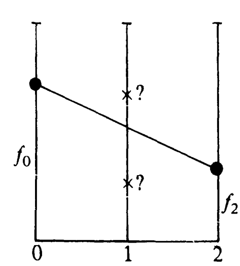


FIGURE 2
$n=2$.

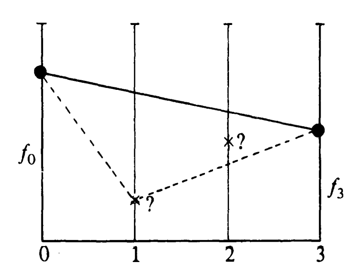


FIGURE 3
$n=3$.

If $n=0$ or 1, the probability is 1. If $n=2$ it is intuitively $1/2$, but if $n=3$, the best our intuition could do was to say "less than $1/4$" (it's not enough just to take the points f_1 and f_2 below the line joining f_0 and f_3). The formal calculations might go:

$$\int_0^1 dx_0 = 1 \qquad \int_0^1 dx_0 \int_0^1 dx_1 = 1$$

$$\int_0^1 dx_0 \int_0^1 dx_2 \int_0^{(x_0+x_2)/2} dx_1 = \int_0^1 dx_0 \int_0^1 \frac{x_0+x_2}{2}\, dx_2 = \int_0^1 \left(\frac{x_0}{2} + \frac{1}{4}\right) dx_0$$

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

$$\int_0^1 dx_0 \int_0^1 dx_3 \int_0^{(2x_0+x_3)/3} dx_1 \int_0^{(x_1+x_3)/2} dx_2$$

$$= \int_0^1 dx_0 \int_0^1 dx_3 \int_0^{(2x_0+x_3)/3} \frac{x_1+x_3}{2}\, dx_1$$

$$= \int_0^1 dx_0 \int_0^1 \left| \frac{x_1^2}{4} + \frac{x_1 x_3}{2} \right|_{x_1=0}^{(2x_0+x_3)/3} dx_3$$

$$= \int_0^1 dx_0 \int_0^1 \left(\frac{2x_0+x_3}{3}\right)\left(\frac{2x_0+x_3}{12} + \frac{x_3}{2}\right) dx_3$$

$$= \frac{1}{36} \int_0^1 dx_0 \int_0^1 \left(4x_0^2 + 16x_0x_3 + 7x_3^2\right) dx_3$$

$$= \frac{1}{36} \int_0^1 \left(4x_0^2 + 8x_0 + \frac{7}{3}\right) dx_0 = \frac{1}{36}\left(\frac{4}{3} + 4 + \frac{7}{3}\right) = \frac{23}{108}.$$

The answer for $n = 3$ is a bit less than a quarter, and quite plausible, but it's easy to make mistakes. In fact we've made one! Can you find it? The lower terminal in the x_2 integration is not necessarily zero. Convexity demands that $x_2 \geqslant x_1 - x_0$, which may be positive, so the lower terminal should be $\max(0, 2x_1 - x_2)$, and the calculations become even more messy than we've indicated. We eventually decided that these are the first few correct answers:

$n =$	0	1	2	3	4	5
	1	1	$\frac{1}{2}$	$\frac{5}{36}$	$\frac{7}{288}$	$\frac{7}{2400}$.

Factorials twice appeared naturally in the denominators, once from the repeated integrations, and once via the fractions in the extremal values occurring in the terminals of the integrals. So we wrote them

$$\frac{1}{(0!)^2} \quad \frac{1}{(1!)^2} \quad \frac{2}{(2!)^2} \quad \frac{5}{(3!)^2} \quad \frac{14}{(4!)^2} \quad \frac{42}{(5!)^2}.$$

The Catalan numbers in the numerators were all-convincing, but how to prove the general formula $c_n/(n!)^2$? The fact that c_n satisfies the convolution 4 was very suggestive. Our investigation was convoluted, but not convolved, in that we never directly invoke property 4. The final undramatic appearance of the Catalan numbers was via the divisibility property 2.

If you chop a convex function in two, the pieces are separately convex (FIGURE 4). But if you join two convex functions, the result needn't be convex (FIGURE 5). But if you join them at the lowest point, you're in business. Start again: write $f_0 = a$, $f_n = b$, $\min f_k = c$, and assume $1 \geqslant a \geqslant b \geqslant c \geqslant 0$. In taking $a \geqslant b$ we lose symmetry, so, if $b > a$, renumber the points from n to 0, and double the final answer.

Is the lowest point unique? Not necessarily! It's clear you can't have two *separate* minima, since this would contradict convexity. But c *could* be attained by several *consecutive* values. When we say monotonic decreasing (or monotonic increasing) we don't mean this *strictly*. The values could remain constant for a while; though convexity demands that this can happen only among the last (or first) several values.

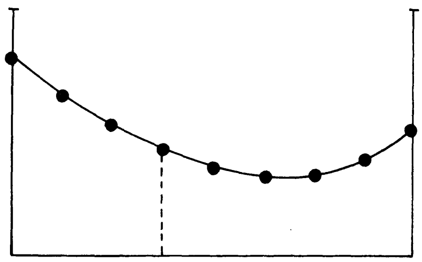


FIGURE 4
Parts of a convex function are convex.

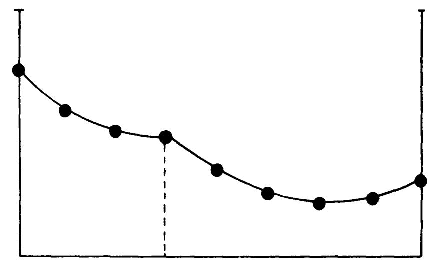


FIGURE 5
The join of two convex functions is not necessarily convex.

We'll calculate $P(n+1)$, the probability that the $n+1$ points form a convex function, by first calculating the probability, $P(k+1; a, c)$, that $k+1$ points, the first one $(0, a)$, the last one (k, c) form a *monotonic decreasing* convex function (FIGURE 6).

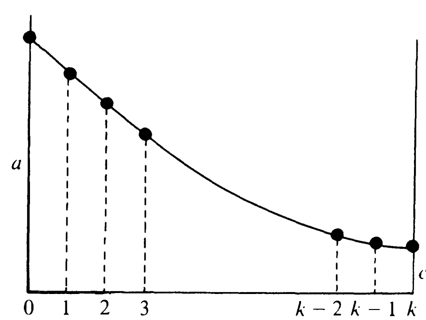


FIGURE 6
A monotonic decreasing convex function.

Then let k run from 1 to $n-1$ and note (FIGURE 7) that the last $n-k+1$ points form a monotonic increasing convex function with probability $P(n-k+1; b, c)$, reading backwards from the point (n, b) to the point (k, c). In case the minimum occurs at the right end, $(k=n, c=b)$, we must also throw in the probability $P(n+1; a, b)$ (recall that we threw away the symmetry by assuming that $a \geqslant b$).

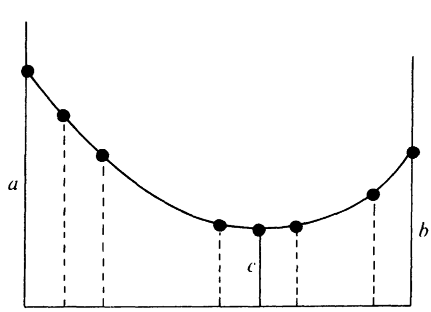


FIGURE 7
A convex function is the join of monotonic decreasing and monotonic increasing ones.

Then

$$P(n+1) = 2\int_0^1 da \int_0^a db \left[P(n+1; a, b) + \int_0^b \left\{ \sum_{k=1}^{n-1} P(k+1; a, c) P(n-k+1; b, c) \right\} dc \right].$$

It remains to calculate $P(k+1; a, c)$, evaluate the sum and perform the integrals. The first turns out to be easy, though quite hard to visualize, unless you are good at seeing things in three or more dimensions. It is the volume of a $(k-1)$-dimensional simplex. We'll do the case $k = 4$ (5 points, 3 dimensions) in detail, to help you get the picture (FIGURES 8 and 9).

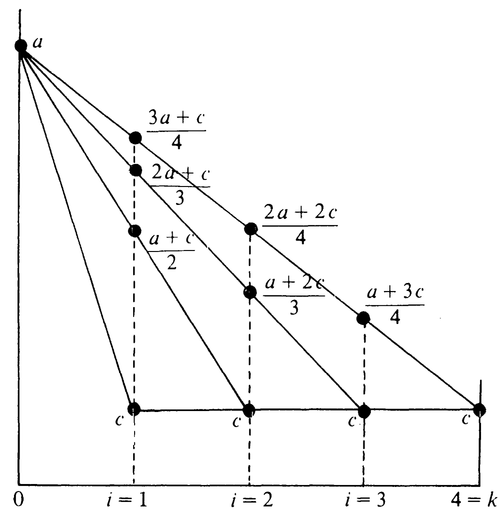


FIGURE 8
The $(k = 4)$ convex monotonic decreasing extremal functions.

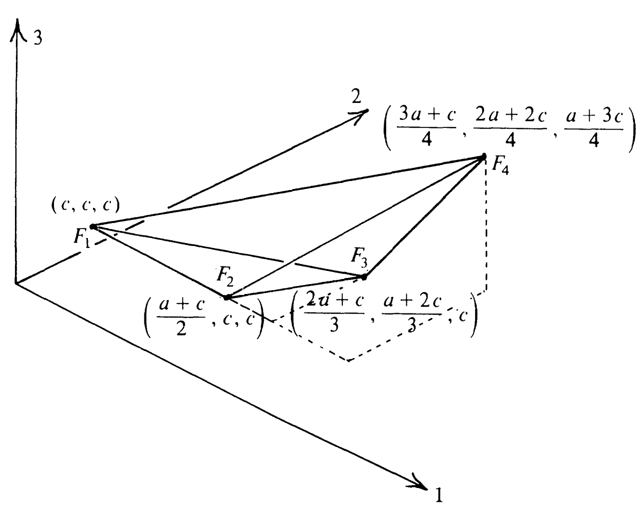


FIGURE 9
The simplex whose vertices are the extremal functions of Fig. 8.

The vertices of the simplex have $k-1$ ($=3$ in our example) coordinates, namely the $k-1$ intermediate values, at $i=1,2,\dots,k-1$, of the k **extremal functions**, F_i, $1 \leqslant i \leqslant k$, each starting at $(0,a)$ and finishing at (k,c). For $k=4$, FIGURE 8 exhibits these as

$$(c,c,c),((a+c)/2,c,c),((2a+c)/3,(a+2c)/3,c),$$
$$((3a+c)/4,(2a+2c)/4,(a+3c))$$

and FIGURE 9 shows the corresponding 3-dimensional simplex. Its base is the triangle $F_1F_2F_3$, with

$$F_1F_2 = \frac{a+c}{2} - c = \frac{a-c}{2},$$

and perpendicular from F_3 onto F_1F_2 equal to

$$\frac{a+2c}{3} - c = \frac{a-c}{3};$$

while its height is

$$\frac{a+3c}{4} - c = \frac{a-c}{4}.$$

The volume is $1/3$ (base $\times$ height), i.e.,

$$\frac{1}{3}\left(\frac{1}{2}\cdot\frac{a-c}{2}\cdot\frac{a-c}{3}\right)\frac{a-c}{4} = \frac{1}{3!}\,\frac{(a-c)^3}{4!}.$$

More generally, the coordinates are

$$\begin{array}{ll}
F_1 & \left(c,\quad c,\quad c,\quad \dots,\quad c,\quad c\right) \\
F_2 & \left(\frac{a+c}{2},\quad c,\quad c,\quad \dots,\quad c,\quad c\right) \\
F_3 & \left(\frac{2a+c}{3},\quad \frac{a+2c}{3},\quad c,\quad \dots,\quad c,\quad c\right) \\
\cdots & \cdots \\
F_{k-1} & \left(\frac{(k-2)a+c}{k-1},\quad \frac{(k-3)a+2c}{k-1},\quad \frac{(k-4)a+3c}{k-1},\quad \dots,\quad \frac{a+(k-2)c}{k-1},\quad c\right) \\
F_k & \left(\frac{(k-1)a+c}{k},\quad \frac{(k-2)a+2c}{k},\quad \frac{(k-3)a+3c}{k},\quad \dots,\quad \frac{2a+(k-2)c}{k},\quad \frac{a+(k-1)c}{k}\right),
\end{array}$$

and the volume of the $(k-1)$-dimensional simplex is (see [4], for example) $1/(k-1)!$ of the determinant got by prefixing a column of ones to these coordinates:

$$\frac{1}{(k-1)!}\begin{vmatrix}
1 & c & c & c & \cdots & c & c \\
1 & \frac{a+c}{2} & c & c & \cdots & c & c \\
1 & \frac{2a+c}{3} & \frac{a+2c}{3} & c & \cdots & c & c \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
1 & \frac{(k-2)a+c}{k-1} & \frac{(k-3)a+2c}{k-1} & \frac{(k-4)a+3c}{k-1} & \cdots & \frac{a+(k-2)c}{k-1} & c \\
1 & \frac{(k-1)a+c}{k} & \frac{(k-2)a+2c}{k} & \frac{(k-3)a+3c}{k} & \cdots & \frac{2a+(k-2)c}{k} & \frac{a+(k-1)c}{k}
\end{vmatrix}.$$

This is easily calculated by subtracting row one from each of the others, and removing a factor $a-c$ from each of rows two to k:

$$\frac{(a-c)^{k-1}}{(k-1)!}\begin{vmatrix} 1 & c & c & c & \dots & c & c \\ 0 & \frac{1}{2} & 0 & 0 & \dots & 0 & 0 \\ 0 & \frac{2}{3} & \frac{1}{3} & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \frac{k-2}{k-1} & \frac{k-3}{k-1} & \frac{k-4}{k-1} & \dots & \frac{1}{k-1} & 0 \\ 0 & \frac{k-1}{k} & \frac{k-2}{k} & \frac{k-3}{k} & \dots & \frac{2}{k} & \frac{1}{k} \end{vmatrix} = \frac{(a-c)^{k-1}}{(k-1)!}\cdot\frac{1}{k!}.$$

With hindsight, we could have saved the printer a great many a's and c's by taking $a=1, c=0$, and then making an affine transformation, squashing the interval $[0,1]$ to $[c,a]$ in each of the $k-1$ dimensions.

The sum $\Sigma_{k=1}^{n-1}P(k+1;a,c)P(n-k+1;b,c)$ is thus

$$\sum_{k=1}^{n-1}\frac{(a-c)^{k-1}(b-c)^{n-k-1}}{k!(k-1)!(n-k)!(n-k-1)!}$$
$$=\frac{1}{((n-1)!)^2}\sum_{k=1}^{n-1}\binom{n-1}{k-1}(a-c)^{k-1}\binom{n-1}{n-k-1}(b-c)^{n-k-1}.$$

This is reminiscent of Leibniz's theorem for the repeated differentiation of a product. Indeed, on looking at Gould's collection of combinatorial identities, it turns out to be the Jacobi polynomial [**6**, #3.131]:

$$\frac{(a-b)^{n-2}}{((n-1)!)^2}\sum_{k=1}^{n-1}\binom{n-1}{k-1}\left(\frac{a-c}{a-b}\right)^{k-1}\binom{n-1}{n-k-1}\left(\frac{b-c}{a-b}\right)^{n-k-1}$$
$$=\frac{(a-b)^{n-2}}{((n-1)!)^2 2^{n-2}(n-2)!}\,\frac{1}{x^2-1}D_x^{n-2}\left\{(x^2-1)^{n-1}\right\}$$

with $x=(a+b-2c)/(a-b)$.

Presumably a good technician could now show that

$$P(n+1;a,b)+\int_0^b\sum_{k=1}^{n-1}P(k+1;a,c)P(n-k+1;b,c)\,dc$$
$$=\frac{1}{n!(n-1)!}\sum_{k=0}^{n-1}\binom{n-1}{k}b^k\binom{n-1}{n-k-1}a^{n-k-1}$$

whose integral from 0 to a with respect to b is

$$\frac{a^n}{(n!)^2}\sum_{k=1}^{n}\binom{n}{k}\binom{n-1}{n-k}.$$

The sum is a Vandermonde convolution, the coefficient of y^n in the expansion of $(1+y)^n(y+1)^{n-1}=(1+y)^{2n-1}$, i.e., $\binom{2n-1}{n}$, so

$$P(n+1) = 2\int_0^1 \frac{a^n}{(n!)^2}\binom{2n-1}{n}\,da = \frac{2}{(n!)^2}\frac{(2n-1)!}{(n+1)n!(n-1)!} = \frac{1}{(n!)^2}\frac{1}{n+1}\binom{2n}{n}$$
$$= \frac{c_n}{(n!)^2},$$

where c_n is the nth Catalan number (property 2 in our list).

This almost proof adds to our deep conviction that we know the answer. But surely we can do the manipulation better?

Any convex function attains its minimum, c say, at one (at least) of the points $k = 0, 1, \dots, n$. So, much more simply,

$$P(n+1) = \int_0^1 \sum_{k=0}^{n} P(k+1;c)P(n-k+1;c)\,dc,$$

where $P(k+1;c)$ is the probability that the function is convex and decreasing to (k,c):

$$P(k+1;c) = \int_{a=c}^{1} P(k+1;a,c)\,da = \int_c^1 \frac{(a-c)^{k-1}\,da}{k!(k-1)!} = \frac{1}{(k!)^2}(a-c)^k\Big|_{a=c}^{a=1}$$
$$= \frac{(1-c)^k}{(k!)^2}$$
$$P(n+1) = \int_0^1 \sum_{k=0}^{n} \frac{(1-c)^k}{(k!)^2}\frac{(1-c)^{n-k}}{((n-k)!)^2}dc = \frac{1}{(n!)^2}\sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k}\int_0^1 (1-c)^n\,dc$$
$$= \frac{1}{(n!)^2}\binom{2n}{n}\frac{1}{n+1} = \frac{c_n}{(n!)^2}.$$

Easy when you know how! But surely there's a neatly convolved proof sitting out there somewhere, which makes direct use of property 4. How do you weave in the factorials? What's the exponential *generating* function,

$$\sum_{k=0}^{\infty} c_n x^n/n!$$

for the Catalan numbers? Does the function $\sum_{k=0}^{\infty} c_n x^n/(n!)^2$ make any sense?

Although we implied at the outset that we were going to reveal all, there's still a great deal that we swept under the rug. J. van de Lune originally submitted the problem to the Unsolved Problems section of the *Amer. Math. Monthly*. It was refereed by several people, including Ernie Enns, who gave us a good start with solving the problem. He observed that the answer could be written

$$P(n+1) = \int_0^1 dx_1 \prod_{k=1}^{n} \int_{\max(0,2x_k - x_{k-1})}^{(1+(n-k)x_k)/(n-k-1)} dx_{k+1},$$

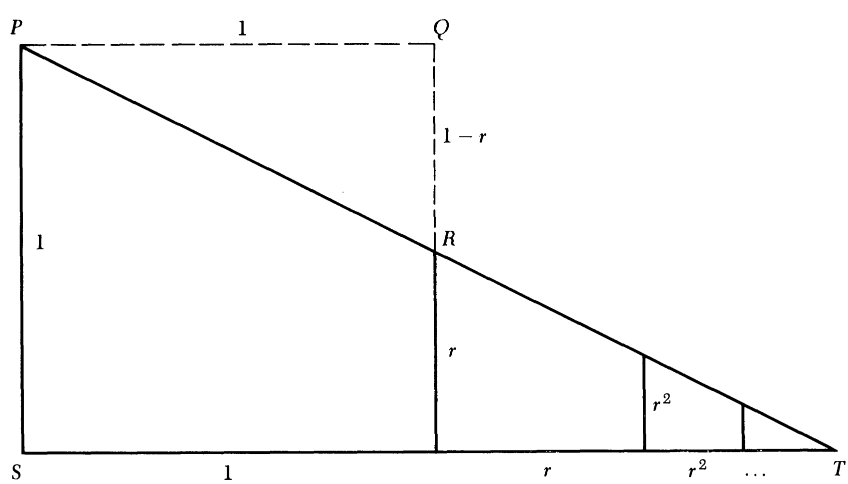
where $n \geqslant 2$ and the lower terminal of the integral for $k = 1$ is 0. He calculated this as far as $n = 4$ (5 points), but, just as we did, managed to get the wrong answers, and different ones, too!

We are further indebted to *Math. Mag.* referees for improving the exposition. The first author thanks the Department of Mathematics and Statistics, The University of Calgary, for hospitality, provision of facilities and a stimulating mathematical environment during his study leave. The second author benefits from a grant from the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

1. William G. Brown, Historical note on a recurrent combinatorial problem, *Amer. Math. Monthly* 72 (1965), 973–977.
2. Louis Comtet, *Advanced Combinatorics*, D. Reidel, Dordrecht, 1974, pp. 52–54, 74, 82.
3. J. H. Conway and H. S. M. Coxeter, Triangulated polygons and frieze patterns, *Math. Gaz.* 57 (1973), 87–94, 175–183; MR 57 #1254-5.
4. John B. Fraleigh and Raymond Beauregard, *Linear Algebra*, Addison-Wesley, 1987, section 5.6.
5. Martin Gardner, Mathematical Games, Catalan numbers: an integer sequence that materializes in unexpected places, *Scientific Amer.* 234, No. 6 (June, 1976), 120–125, 132.
6. Henry W. Gould, *Combinatorial Identities*, revised ed., Morgantown, WV, 1972, MR 50 #6879.
7. Henry W. Gould, Research bibliography of two special number sequences (Catalan and Bell numbers), *Math. Monongaliae*, 12, Morgantown, WV, 1971; sixth ed., 1985, MR 43 #4755, 53 #5460.
8. Mike Kuchinski, *Catalan Structures and Correspondences*, M.Sc. thesis, W. Virginia Univ., May 1977. [References 6 to 8 are available from Dept. of Math., W. Virginia Univ., Morgantown, WV 26506.]
9. Fred S. Roberts, *Applied Combinatorics*, Prentice-Hall, 1984, pp. 234–243.
10. N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, 1973, sequence 557, and pp. 18–20.

Proof Without Words



$\triangle PQR \approx \triangle TSP.$

$$\therefore 1 + r + r^2 + \cdots = \frac{1}{1-r}.$$

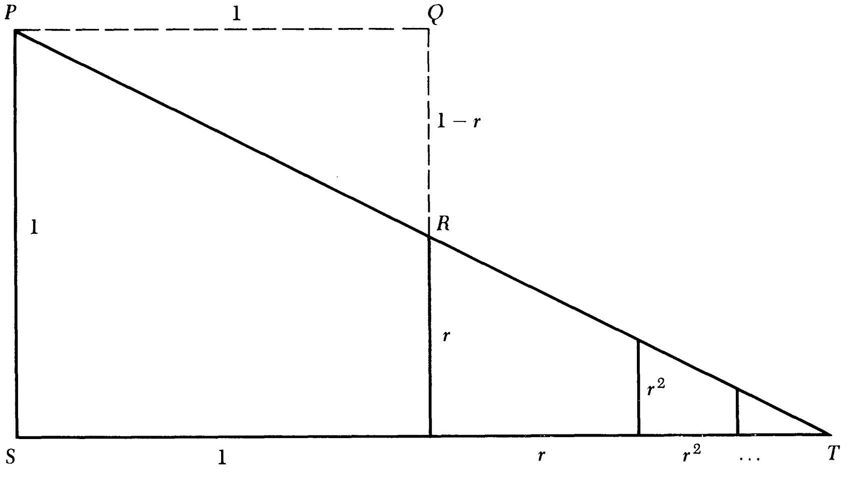
–BENJAMIN G. KLEIN
IRL C. BIVENS
DAVIDSON COLLEGE
DAVIDSON, NC 28036

and a stimulating mathematical environment during his study leave. The second author benefits from a grant from the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

1. William G. Brown, Historical note on a recurrent combinatorial problem, *Amer. Math. Monthly* 72 (1965), 973–977.
2. Louis Comtet, *Advanced Combinatorics*, D. Reidel, Dordrecht, 1974, pp. 52–54, 74, 82.
3. J. H. Conway and H. S. M. Coxeter, Triangulated polygons and frieze patterns, *Math. Gaz.* 57 (1973), 87–94, 175–183; MR 57 #1254-5.
4. John B. Fraleigh and Raymond Beauregard, *Linear Algebra*, Addison-Wesley, 1987, section 5.6.
5. Martin Gardner, Mathematical Games, Catalan numbers: an integer sequence that materializes in unexpected places, *Scientific Amer.* 234, No. 6 (June, 1976), 120–125, 132.
6. Henry W. Gould, *Combinatorial Identities*, revised ed., Morgantown, WV, 1972, MR 50 #6879.
7. Henry W. Gould, Research bibliography of two special number sequences (Catalan and Bell numbers), *Math. Monongaliae*, 12, Morgantown, WV, 1971; sixth ed., 1985, MR 43 #4755, 53 #5460.
8. Mike Kuchinski, *Catalan Structures and Correspondences*, M.Sc. thesis, W. Virginia Univ., May 1977. [References 6 to 8 are available from Dept. of Math., W. Virginia Univ., Morgantown, WV 26506.]
9. Fred S. Roberts, *Applied Combinatorics*, Prentice-Hall, 1984, pp. 234–243.
10. N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, 1973, sequence 557, and pp. 18–20.

Proof Without Words



$\triangle PQR \approx \triangle TSP.$

$$\therefore 1 + r + r^2 + \cdots = \frac{1}{1-r}.$$

–BENJAMIN G. KLEIN
IRL C. BIVENS
DAVIDSON COLLEGE
DAVIDSON, NC 28036

The Centrality of Mathematics in the History of Western Thought*

JUDITH V. GRABINER
Pitzer College
Claremont, CA 91711

1. Introduction Since this paper was first given to educators, let me start with a classroom experience. It happened in a course in which my students had read some of Euclid's *Elements of Geometry*. A student, a social science major, said to me, "I never realized mathematics was like this. Why, it's like philosophy!" That is no accident, for philosophy is like mathematics. When I speak of the centrality of mathematics in western thought, it is this student's experience I want to recapture—to reclaim the context of mathematics from the hardware store with the rest of the tools and bring it back to the university. To do this, I will discuss some major developments in the history of ideas in which mathematics has played a central role.

I do not mean that mathematics has by itself caused all these developments; what I do mean is that mathematics, whether causing, suggesting, or reinforcing, has played a key role; it has been there, at center stage. We all know that mathematics has been the language of science for centuries. But what I wish to emphasize is the crucial role of mathematics in shaping views of man and the world held not just by scientists, but by everyone educated in the western tradition.

Given the vastness of that tradition, I will give many examples only briefly, and be able to treat only a few key illustrative examples at any length. Sources for the others may be found in the bibliography. (See also [**26**].)

Since I am arguing for the centrality of mathematics, I will organize the paper around the key features of mathematics which have produced the effects I will discuss. These features are the certainty of mathematics and the applicability of mathematics to the world.

2. Certainty For over two thousand years, the certainty of mathematics, particularly of Euclidean geometry, has had to be addressed in some way by any theory of knowledge. Why was geometry certain? Was it because of the subject matter of geometry, or because of its method? And what were the implications of that certainty?

Even before Euclid's monumental textbook, the philosopher Plato saw the certainty of Greek geometry—a subject which Plato called "knowledge of that which always is" [**41**, 527b]—as arising from the eternal, unchanging perfection of the objects of mathematics. By contrast, the objects of the physical world were always coming into being or passing away. The physical world changes, and is thus only an approximation to the higher ideal reality. The philosopher, then, to have his soul drawn from the changing to the real, had to study mathematics. Greek geometry fed Plato's idealistic philosophy; he emphasized the study of Forms or Ideas transcending experience: the idea of justice, the ideal state, the idea of the Good. Plato's views were used by philosophers within the Jewish, Christian, and Islamic traditions to deal with how a divine being, or souls, could interact with the material world [**46**, pp. 382–3] [**51**, pp. 17–40] [**34**, p. 305ff] [**23**, p. 46–67]. For example, Plato's account of the creation of the world in his *Timaeus*, where a god makes the physical universe by copying an

*©International Congress of Mathematicians, 1986, Berkeley, California

ideal mathematical model, became assimilated in early Christian thought to the Biblical account of creation [29, pp. 21–22]. One finds highly mathematicized cosmologies, influenced by Plato, in the mystical traditions of Islam and Judaism as well. The tradition of Platonic Forms or Ideas crops up also in such unexpected places as the debates in eighteenth- and nineteenth-century biology over the fixity of species. Linnaeus in the eighteenth, and Louis Agassiz in the nineteenth century seem to have thought of species as ideas in the mind of God [16, p. 34] [13, pp. 36–7]. When we use the common terms "certain" and "true" outside of mathematics, we use them in their historical context, which includes the long-held belief in an unchanging reality—a belief stemming historically from Plato, who consistently argued for it using examples from mathematics.

An equally notable philosopher, who lived just before Euclid, namely Aristotle, saw the success of geometry as stemming, not from perfect eternal objects, but instead from its method [*Posterior Analytics*, I 10–11; I 1–2 (77a5, 71b ff)] [19, vol. I, Chapter IX]. The certainty of mathematics for Aristotle rested on the validity of its logical deductions from self-evident assumptions and clearly-stated definitions. Other subjects might come to share that certainty if they could be understood within the same logical form; Aristotle, in his *Posterior Analytics*, advocated reducing all scientific discourse to syllogisms, that is, to logically-deduced explanations from first principles. In this tradition, Archimedes proved the law of the lever, not by experiments with weights, but from deductions *à la* Euclid from postulates like "equal weights balance at equal distances" [18, pp. 189–194]. Medieval theologians tried to prove the existence of God in the same way. This tradition culminates in the 1675 work of Spinoza, *Ethics Demonstrated in Geometrical Order*, with such axioms as "That which cannot be conceived through another must be conceived through itself," definitions like "By substance I understand that which is in itself and conceived through itself" (compare Euclid's "A point is that which has no parts"), and such propositions as "God or substance consisting of infinite attributes... necessarily exists," whose proof ends with a QED [48, pp. 41–50]. Isaac Newton called his famous three laws "Axioms, or Laws of Motion." His *Principia* has a Euclidean structure, and the law of gravity appears as Book III, Theorems VII and VIII [37, pp. 13–14, pp. 414–17]. The Declaration of Independence of the United States is one more example of an argument whose authors tried to inspire faith in its certainty by using the Euclidean form. "We hold these truths to be self-evident..." not that all right angles are equal, but "that all men are created equal." These self-evident truths include that if any government does not obey these postulates, "it is the right of the people to alter or abolish it." The central section begins by saying that they will "prove" King George's government does not obey them. The conclusion is "We, *therefore*... declare, that these United Colonies are, and of right ought to be, free and independent states." (My italics) (Jefferson's mathematical education, by the way, was quite impressive by the standards of his time.)

Thus a good part of the historical context of the common term "proof" lies in Euclidean geometry—which was, I remind you, a central part of Western education.

However, the certainty of mathematics is not limited to Euclidean geometry. Between the rise of Islamic culture and the eighteenth century, the paradigm governing mathematical research changed from a geometric one to an algebraic, symbolic one. In algebra even more than in the Euclidean model of reasoning, the method can be considered independently of the subject-matter involved. This view looks at the method of mathematics as finding truths by manipulating symbols. The approach first enters the western world with the introduction of the Hindu-Arabic number system in the twelfth-century translations into Latin of Arabic mathematical works, notably al-Khowarizmi's algebra. The simplified calculations using the Hindu-Arabic numbers were called the "method of al-Khowarizmi" or as Latinized "the method of algorism" or algorithm.

In an even more powerful triumph of the heuristic power of notation, François Viète in 1591 introduced literal symbols into algebra: first, using letters in general to stand for any number in the theory of equations; second, using letters for any number of unknowns to solve word problems [4, pp. 59–63, 65]. In the seventeenth century, Leibniz, struck by the heuristic power of arithmetical and algebraic notation, invented such a notation for his new science of finding differentials—an algorithm for manipulating the d and integral symbols, that is, a calculus (a term which meant to him the same thing as "algorithm" to us). Leibniz generalized the idea of heuristic notation in his philosophy [**30**, pp. 12–25]. He envisioned a symbolic language which would embody logical thought just as these earlier symbolic languages enable us to perform algebraic operations correctly and mechanically. He called this language a "universal characteristic," and later commentators, such as Bertrand Russell, see Leibniz as the pioneer of symbolic logic [**45**, p. 170]. Any time a disagreement occurred, said Leibniz, the opponents could sit down and say "Let us calculate," and—mechanically—settle the question [**30**, p. 15]. Leibniz's appreciation of the mechanical element in mathematics when viewed as symbolic manipulation is further evidenced by his invention of a calculating machine. Other seventeenth-century thinkers also stressed the mechanical nature of thought in general: for instance, Thomas Hobbes wrote "Words are wise men's counters, they do but reckon by them" [**21**, Chapter 4, p. 143]. Others tried to introduce heuristically powerful notation in different fields: consider Lavoisier's new chemical notation which he called a "chemical algebra" [**14**, p. 245].

These successes led the great prophet of progress, the Marquis de Condorcet, to write in 1793 that algebra gives "the only really exact and analytical language yet in existence.... Though this method is by itself only an instrument pertaining to the science of quantities, it contains within it the principles of a universal instrument, applicable to all combinations of ideas" [**9**, p. 238]. This could make the progress of "every subject embraced by human intelligence... as sure as that of mathematics" [**9**, pp. 278–9]. The certainty of symbolic reasoning has led us to the idea of the certainty of progress. Though one might argue that some fields had not progressed one iota beyond antiquity, it was unquestionably true by 1793 that mathematics and the sciences had progressed. To quote Condorcet once more: "the progress of the mathematical and physical sciences reveals an immense horizon... a revolution in the destinies of the human race" [**9**, p. 237]. Progress was possible; why not apply the same method to the social and moral spheres as well?

No account of attempts to extend the method of mathematics to other fields would be complete without discussing René Descartes, who in the 1630's combined the two methods we have just discussed—that of geometry and that of algebra—into analytic geometry. Let us look at his own description of how to make such discoveries. Descartes depicted the building-up of the deductive structure of a science—proof—as a later task than analysis or discovery. One first needed to analyze the whole into the correct "elements" from which truths could later be deduced. "The first rule," he wrote in his *Discourse on Method*, "was never to accept anything as true unless I recognized it to be evidently such... The second was to divide each of the difficulties which I encountered into as many parts as possible, and as might be required for an easier solution..." Then, "the third [rule] was to [start]... with the things which were simplest and easiest to understand, gradually and by degrees reaching toward more complex knowledge" [**10**, Part II, p. 12]. Descartes presented his method as the key to his own mathematical and scientific discoveries. Consider, for instance, the opening line of his *Geometry*: "All problems in geometry can easily be reduced to such terms that a knowledge of the lengths of certain straight lines suffices for their construction. Just as arithmetic is composed of only four or five operations..., so in geometry" [**11**, Book I, p. 3]. Descartes's influence on subsequent philosophy, from Locke's empiricism to Sartre's existentialism, is well known and will not be reviewed here. But for our purposes it is important to note that the thrust of Descartes's argument is that emulating the method successful in mathematical discovery will lead to successful discoveries in other fields [**10**, Part Five].

Descartes' method of analysis fits nicely with the Greek atomic theory, which had been newly revived in the seventeenth century: all matter is the sum of atoms; analyze the properties of the whole as the sum of these parts [**17**, Chapter VIII, esp. p. 217]. Thus the idea of studying something by "analysis" was doubly popular in seventeenth- and eighteenth-century thought. I would like to trace just one line of influence of this analytic method. Adam Smith in his 1776 *Wealth of Nations* analyzed [**47**, p. 12] the competitive success of economic systems by means of the concept of division of labor. The separate elements, each acting as efficiently as possible, provided for the overall success of the manufacturing process; similarly, each individual in the whole economy, while striving to increase his individual advantages, is "led as if by an Invisible Hand to promote ends which were not part of his original intention" [**47**, p. 27]—that is, the welfare of the whole of society. This Cartesian method of studying a whole system by analyzing it into its elements, then synthesizing the elements to produce the whole, was especially popular in France. For instance, Gaspard François de Prony had the job of calculating, for the French Revolutionary government, a set of logarithmic and trigonometric tables. He, himself, said he did it by applying Adam Smith's ideas about the division of labor. Prony organized a group of people into a hierarchical system to compute these tables. A few mathematicians decided which functions to use; competent technicians then reduced the job of calculating the functions to a set of simple additions and subtractions of pre-assigned numbers; and, finally, a large number of low-level human "calculators" carried out the additions and subtractions. Charles Babbage, the early nineteenth-century pioneer of the digital computer, applied the Smith-Prony analysis and embodied it in a machine [**1**, Chapter XIX]. The way Babbage's ideas developed can be found in a chapter in his *Economy of Machinery* entitled "On the Division of Mental Labour" [**1**, Chapter XIX]. Babbage was ready to convert Prony's organization into a computing machine because Babbage had long been impressed by the arguments of Leibniz and his followers on the power of notation to make such mathematical calculation mechanical, and Babbage, like Leibniz, accounted for the success of mathematics by "the accurate simplicity of its language" [**22**, p. 26]. Since Babbage's computer was designed to be "programmed" by punched cards, Hollerith's later invention of punched-card census data processing, twentieth-century computing, and other applications of the Cartesian "divide-and-solve" approach, including top-down programming, are also among the offspring of Descartes's mathematically-inspired method.

Whatever view of the *cause* of the certainty of mathematics one adopts, the *fact* of certainty in itself has had consequences. The "fact of mathematical certainty" has been taken to show that there exists *some* sort of knowledge, and thus to refute skepticism. Immanuel Kant in 1783 used such an argument to show that metaphysics is possible [**25**, Preamble, Section IV]. If metaphysics exists, it is independent of experience. Nevertheless, it is not a complex of tautologies. Metaphysics, for Kant, had to be what he called "synthetic," giving knowledge based on premises which is not obtainable simply by analyzing the premises logically. Is there such knowledge? Yes, said Kant, look at geometry. Consider the truth that the sum of the angles of a triangle is two right angles. We do not get this truth by analyzing the concept of triangle—all that gives us, Kant says, is that there are three angles. To gain the knowledge, one must make a construction: draw a line through one vertex parallel to the opposite side. (I now leave the proof as an exercise.) The construction is essential; it takes place in space, which Kant sees as a unique intuition of the intellect. (This example [**24**, II "Method of Transcendentalism," Chapter I, Section I, p. 423] seems to require the space to be Euclidean; I will return to this point later on.) Thus synthetic knowledge independent of experience *is* possible, so metaphysics—skeptics like David Hume to the contrary—is also possible.

This same point—that mathematics is knowledge, so there *is* objective truth—has been made throughout history, from Plato's going beyond Socrates' agnostic critical method, through George Orwell's hero, Winston Smith, attempting to assert, in the face of the totalitarian state's overwhelming power over the human intellect, that two and two are four.

Moreover, since mathematics is certain, perhaps we can, by examining mathematics, find which properties *all* certain knowledge must have. One such application of the "fact of mathematical certainty" was its use to solve what in the sixteenth century was called the problem of the criterion [**43**, Chapter I]. If there is only one system of thought around, people might well accept that one as true—as many Catholics did about the teachings of the Church in the Middle Ages. But then the Reformation developed alternative religious systems, and the Renaissance rediscovered the thought of pagan antiquity. Now the problem of finding the criterion that identified the true system became acute. In the seventeenth and eighteenth centuries, many thinkers looked to mathematics to help find an answer. What was the sign of the certainty of the conclusions of mathematics? The fact that nobody disputed them [**43**, Chapter VII]. Distinguishing mathematics from religion and philosophy, Voltaire wrote, "There are no sects in geometry. One does not speak of a Euclidean, an Archimedean" [**49**, Article "Sect."]. What every reasonable person agrees upon—that is the truth. How can this be applied to religion? Some religions forbid eating beef, some forbid eating pork; therefore, since they disagree, they both are wrong. But, continues Voltaire, all religions agree that one should worship God and be just; that must therefore be true. "There is but one morality," says Voltaire, "as there is but one geometry" [**49**, Miscellany, p. 225].

3. Applicability Let us turn now from the certainty of mathematics to its applicability. Since applying mathematics to describe the world works so well, thinkers who reflect on the applicability of mathematics find that it affects their views not only about thought, but also about the world. For Plato, the applicability of mathematics occurs because this world is merely an approximation to the higher mathematical reality; even the motions of the planets were inferior to pure mathematical motions [**41**, 529d]. For Aristotle, on the other hand, mathematical objects are just abstracted from the physical world by the intellect. A typical mathematically-based science is optics, in which we study physical objects—rays of light—as though they were mathematical straight lines [*Physics* II, Chapter 2; 194a]. We can thus use all the tools of geometry in that science of optics, but it is the light that is real.

One might think that Plato is a dreamer and Aristotle a hard-headed practical man.

But today's engineer steeped in differential equations is the descendant of the dreamer. From Plato—and his predecessors the Pythagoreans who taught that "all is number"—into the Renaissance, many thinkers looked for the mathematical reality beyond the appearances. So did Copernicus, Kepler, and Galileo [**7**, Chapters 3, 5, 6]. The Newtonian world-system that completed the Copernican revolution was embodied in a mathematical model, based on the laws of motion and inverse-square gravitation, and set in Platonically absolute space and time ([**6**]; cf. [**7**, Chapter 7]). The success of Newtonian physics not only strongly reinforced the view that mathematics was the appropriate language of science, but also strongly reinforced the emerging ideas of progress and of truth based on universal agreement.

Another consequence of the Newtonian revolution was Newton's explicit help to theology, strongly buttressing what was called the argument for God's existence from design. The mathematical perfection of the solar system—elliptical orbits nearly circular, planets moving all in the same plane and direction—could not have come about by chance, said Newton, but "from the counsel and dominion of an intelligent and powerful Being" [**37**, General Scholium, p. 544]. "Natural theology," as this doctrine was called, focussed on examples of design and adaptation in nature, inspiring considerable research in natural history, especially on adaptation, research which was to play a role in Darwin's discovery of evolution by natural selection [**14**, pp. 263–266].

Just as the "fact of mathematical certainty" made certainty elsewhere seem achievable, so the "fact of mathematical applicability" in physical science inspired the pioneers of the idea of social science, Auguste Comte and Adolphe Quetelet. Both Comte and Quetelet were students of mathematical physics and astronomy in the early nineteenth century; Comte, while a student at the École polytechnique in Paris, was particularly inspired by Lagrange, Quetelet, and Laplace. Lagrange's great *Analytical Mechanics* was an attempt to reduce all of mechanics to mathematics. Comte went further: if physics was built on mathematics, so was chemistry built on physics, biology on chemistry, psychology on biology, and finally his own new creation, sociology (the term is his) would be built on psychology [**8**, Chapter II]. The natural sciences were no longer (as they had once been) theological or metaphysical; they were what Comte called "positive"—based only on observed connections between things. Social science could now also become positive. Comte was a reformer, hoping for a better society through understanding what he called "social physics." His philosophy of positivism influenced twentieth-century logical positivism, and his ideas on history—"social dynamics"—influenced Feuerbach and Marx [**32**, Chapter 4]. Still, Comte only prophesied but did not create quantitative social science; this was done by Quetelet.

For Quetelet's conception of quantitative social science, the fact of applicability of mathematics was crucial. "We can judge of the perfection to which a science has come," he wrote in 1828, "by the ease with which it can be approached by calculation" (quoted in [**27**, p. 250]). Quetelet noted that Laplace had used probability and statistics in determining planetary orbits; Quetelet was especially impressed by what we call the normal curve of errors. Quetelet found empirically that many human traits—height, for instance—gave rise to a normal curve. From this, he defined the statistical concept, and the term, "average man" (*homme moyen*). Quetelet's work demonstrates that, just as the Platonic view that geometry underlies reality made mathematical physics possible, so having a statistical view of data is what makes social science possible.

Quetelet found also that many social statistics—the number of suicides in Belgium, for instance, or the number of murders—produced roughly the same figures every year. The constancy of these rates over time, he argued, dictated that murder or suicide had constant social causes. Quetelet's discovery of the constancy of crime rates raised an urgent question: whether the individuals are people or particles, do statistical laws say anything about individuals? or are the individuals free?

Laplace, recognizing that one needed probability to do physics, said that this fact did not mean that the laws governing the universe were ultimately statistical. In ignorance of the true causes, Laplace said, people thought that events in the universe depended on chance, but in fact all is determined. To an infinite intelligence which could comprehend all the forces in nature and the "respective situation of the beings who composed it," said Laplace, "nothing would be uncertain" [**28**, Chapter II]. Similarly, Quetelet held that "the social state prepares these crimes, and the criminal is merely the instrument to execute them" [**27**].

Another view was held by James Clerk Maxwell. In his work on the statistical mechanics of gases, Maxwell argued that statistical regularities in the large told you nothing about the behavior of individuals in the small [**33**, Chapter 22, pp. 315–16]. Maxwell seems to have been interested in this point because it allowed for free will. And this argument did not arise from Maxwell's physics; he had read and pondered the work of Quetelet on the application of statistical thinking to society [**44**]. The same sort of dispute about the meaning of probabilistically-stated laws has of course recurred in the twentieth-century philosophical debates over the foundations of quantum mechanics.

Thus discussions of basic philosophical questions—is the universe an accident or a divine design? is there free will or are we all programmed?—owe surprisingly much to the applicability of mathematics.

4. More than one geometry? Given the centrality of mathematics to western thought, what happens when prevailing views of the nature of mathematics change? Other things must change too. Since geometry had been for so long the canonical example both of the certainty and of the applicability of mathematics, the rise of non-Euclidean geometry was to have profound effects.

As is well known, in attempts to prove Euclid's parallel postulate and thus, as Saccheri put it in 1733, remove the single blemish from Euclid, mathematicians deduced a variety of surprising consequences from denying that postulate. Gauss, Bolyai, and Lobachevsky in the early nineteenth century each separately recognized that these consequences were not absurd, but rather were valid results in a consistent, non-Euclidean (Gauss's term) geometry.

Recall that Kant had said that space (by which he meant Euclidean 3-space) was the form of all our perceptions of objects. Hermann von Helmholtz, led in mid-century to geometry by his interest in the psychology of perception, asked whether Kant might be wrong: could we imagine ordering our perceptions in a non-Euclidean space? Yes, Helmholtz said. Consider the world as reflected in a convex mirror. Thus, the question of which geometry describes the world is no longer a matter for intuition —or for self-evident assumptions—but for *experience* [**20**].

What did this view—expressed as well by Bernhard Riemann and W. K. Clifford, among others—do to the received accounts of the relation between mathematics and the world? It detached mathematics from the world. Euclidean and non-Euclidean geometry give the first clear-cut historical example of two mutually contradictory mathematical structures, of which at most one can actually represent the world. This seems to indicate that the choice of mathematical axioms is one of intellectual freedom, not empirical constraint; this view, reinforced by Hamilton's discovery of a non-commutative algebra, suggested that mathematics is a purely formal structure, or as Benjamin Peirce put it, "Mathematics is the science which draws necessary conclusions," [**40**]—*not* the science of number (even symbolic algebra had been just a generalized science of number) or the science of space. Now that the axioms were no longer seen as necessarily deriving from the world, the applicability of mathematics to the world became turned upside down. The world is no longer, as it was for Plato, an imperfect model of the true mathematical reality; instead, mathematics provides a set of different models for one empirical reality. In 1902 the physicist Ludwig Boltzmann expressed a view which had become widely held: that models, whether physical or mathematical, whether geometric or statistical, had become the means by which the sciences "comprehend objects in thought and represent them in language" [**3**]. This view, which implies that the sciences are no longer claiming to speak directly about reality, is now widespread in the social sciences as well as the natural sciences, and has transformed the philosophy of science. As applied to mathematics itself—the formal model of mathematical reasoning—it has resulted in Gödel's demonstration that one can never prove the consistency of mathematics, and the resulting conclusion among some philosophers that there is no certainty anywhere, not even in mathematics [**2**, p. 206].

5. Opposition The best proof of the centrality of mathematics is that every example of its influence given so far has provoked strong and significant opposition. Attacks on the influence of mathematics have been of three main types. Some people have simply favored one view of mathematics over other views; other people have granted the importance of mathematics but have opposed what they consider its overuse or extension into inappropriate domains; still others have attacked mathematics, and often all of science and reason, as cold, inhuman, or oppressive.

Aristotle's reaction against Platonism is perhaps the first example of opposition to one view of mathematics (eternal objects) while championing another (deductive method). Another example is Newton's attack on Descartes's attempt to use nothing but "self-evident" assumptions to figure out how the universe worked. There are many mathematical systems God could have used to set up the world, said Newton. One could not decide *a priori* which occurs; one must, he says, observe in nature which law actually holds. Though mathematics is the tool one uses to discover the laws, Newton concludes that God set up the world by free choice, not mathematical necessity [**35**, pp. 7–8] [**36**, p. 47]. This point is crucial to Newton's natural theology: that the presence of order in nature proves that God exists.

Another example of one view based on mathematics attacking another can be found in Malthus's *Essay on Population* of 1798. He accepts the Euclidean deductive model —in fact he begins with two "postulata": man requires food, and the level of human sexuality remains constant [**31**, Chapter I]. His consequent analysis of the growth of population and of food supply rests on mathematical models. Nonetheless, one of Malthus's chief targets is the predictions by Condorcet and others of continued human progress modelled on that of mathematics and science. As in Newton's attack on Descartes, Malthus applied one view of mathematics to attack the conclusions others claimed to have drawn from mathematics.

Our second category of attacks—drawing a line that mathematics should not cross —is exemplified by the seventeenth-century philosopher and mathematician Blaise Pascal. Reacting against Cartesian rationalism, Pascal contrasted the "esprit géometrique" (abstract and precise thought) with what he called the "esprit de finesse" (intuition) [**39**, *Pensée* 1] holding that each had its proper sphere, but that mathematics had no business outside its own realm. "The heart has its reasons," wrote Pascal, "which reason does not know" [39, *Pensée* 277]. Nor is this contradicted by the fact that Pascal was willing to employ mathematical thinking for theological purposes—recall his "wager" argument to convince a gambling friend to try acting like a good Catholic [39, *Pensée* 233]; the point here was to use his friend's own probabilistic reasoning style in order to convince him to go on to a higher level.

Similarly, the mathematical reductionism of men like Lagrange and Comte was opposed by men like Cauchy. Cauchy, whom we know as the man who brought Euclidean rigor to the calculus, opposed both Lagrange's attempt to reduce mechanics to calculus and calculus to formalistic algebra [15, pp. 51–54], and opposed the positivists' attempt to reduce the human sciences to an ultimately mathematical form. "Let us assiduously cultivate the mathematical sciences," Cauchy wrote in 1821, but "let us not imagine that one can attack history with formulas, nor give for sanction to morality theorems of algebra or integral calculus" [5, p. vii]. Analogously, in our own day, computer scientist Joseph Weizenbaum attacks the modern, computer-influenced view that human beings are nothing but processors of symbolic information, arguing that the computer scientist should "teach the limitations of his tools as well as their power" [50, p. 277].

Finally, we have those who are completely opposed to the method of analysis, the mathematization of nature, and the application of mathematical thought to human affairs. Witness the Romantic reaction against the Enlightenment: Goethe's opposition to the Newtonian analysis of white light, or, even more extreme, William Wordsworth in *The Tables Turned*:

Sweet is the lore which Nature brings;
Our meddling intellect
Mis-shapes the beauteous forms of things:—
We murder to dissect.

Again, Walt Whitman, in his poem "When I heard the learn'd astronomer," describes walking out on the lecture on celestial distances, having become "tired and sick," going outside instead to look "up in perfect silence at the stars."

Reacting against statistical thinking on behalf of the dignity of the individual, Charles Dickens in his 1854 novel *Hard Times* satirizes a "modern school" in which a pupil is addressed as "Girl number twenty" [12, Book I, Chapter II]; the schoolmaster's son betrays his father, justifying himself by pointing out that in any given population a certain percentage will become traitors, so there is no occasion for surprise or blame [12, Book III, Chapter VII]. In a more political point, Dickens through his hero denounces the analytically-based efficiency of industrial division of labor, saying it regards workers as though they were nothing but "figures in a sum" [12, Book II, Chapter V].

The Russian novelist Evgeny Zamyatin, in his early-twentieth-century antiutopian novel *We* (a source for Orwell's *1984*), envisions individuals reduced to being numbers, and mathematical tables of organization used as instruments of social control. Though the certainty of mathematics, and thus its authority, has sometimes been an ally of liberalism, as we have seen in the cases of Voltaire and Condorcet, Zamyatin saw how it could also be used as a way of establishing an unchallengeable authority, as philosophers like Plato and Hobbes had tried to use it, and he wanted no part of it.

6. Conclusion As the battles have raged in the history of Western thought, mathematics has been on the front lines. What does it all (to choose a phrase) add up to?

My point is not that what these thinkers have said about mathematics is right, or is wrong. But this history shows that the nature of mathematics has been—and must be—taken into account by anyone who wants to say anything important about philosophy or about the world. I want, then, to conclude by advocating that we teach mathematics *not* just to teach quantitative reasoning, *not* just as the language of science—though these are very important—but that we teach mathematics to let people know that one cannot fully understand the humanities, the sciences, the world of work, and the world of man without understanding mathematics in its central role in the history of Western thought.

Acknowledgements. I thank the students in my Mathematics 1 classes at Pomona and Pitzer Colleges for stimulating discussions and suggestions on some of the topics covered in this paper, especially David Bricker, Maria Camareña, Marcelo D'Asero, Rachel Lawson, and Jason Gottlieb. I also thank Sandy Grabiner for both his helpful comments and his constant support and encouragement.

REFERENCES

1. Charles Babbage, *On the Economy of Machinery*, Charles Knight, London, 1832.
2. William Barrett, *Irrational Man: A Study in Existential Philosophy*, Doubleday, New York, 1958. Excerpted in William L. Schaaf, ed., *Our Mathematical Heritage*, Collier, New York, 1963.
3. Ludwig Boltzmann, Model, *Encyclopedia Britannica*, 1902.
4. Carl Boyer, *History of Analytic Geometry*, Scripta Mathematica, New York, 1956.
5. A.-L. Cauchy, *Cours d'analyse*, 1821. Reprinted in A.-L. Cauchy, *Oeuvres*, series 2, vol. 3, Gauthier-Villars, Paris, 182.
6. I. Bernard Cohen, *The Newtonian Revolution*, Cambridge University Press, Cambridge, 1980.
7. ______, *The Birth of a New Physics*, 2d edition. W. W. Norton, New York and London, 1985.
8. Auguste Comte, *Cours de philosophie positive*, vol. I, Bachelier, Paris, 1830.
9. Marquis de Condorcet, *Sketch for a Historical Picture of the Progress of the Human Mind*, 1793, tr, June Barraclough. In Keith Michael Baker, ed., *Condorcet: Selected Writings*. Bobbs-Merrill, Indianapolis, 1976.
10. René Descartes, *Discourse on Method*, 1637, tr. L. J. Lafleur, Liberal Arts Press, New York, 1956.
11. ______, *La géométrie*, 1637, tr., D. E. Smith and Marcia L. Latham, *The Geometry of René Descartes*, Dover, NY, 1954.
12. Charles Dickens, *Hard Times*, 1854. Norton Critical Edition edited by George Ford and Sylvere Monod, W. W. Norton, New York and London, 1966.
13. Neal C. Gillespie, *Charles Darwin and the Problem of Creation*, University of Chicago Press, Chicago and London, 1979.
14. Charles C. Gillespie, *The Edge of Objectivity*, Princeton University Press, Princeton, NJ, 1960.
15. Judith V. Grabiner, *The Origins of Cauchy's Rigorous Calculus*, M.I.T. Press, Cambridge, Mass., 1981.
16. John C. Greene, *Science, Ideology, and World View: Essays in the History of Evolutionary Ideas*, University of California Press, Berkeley, 1981.
17. A. Rupert Hall, *From Galileo to Newton*, 1630–1720, Harper and Row, New York and Evanston, 1963.
18. T. L. Heath (Editor), *The Works of Archimedes with the Method of Archimedes*, New York, n.d.
19. ______, *The Thirteen Books of Euclid's Elements*, Volume I, Cambridge University Press, 1925, reprinted by Dover, New York, 1956.
20. Hermann von Helmholtz, On the origin and significance of geometrical axioms, 1870, reprinted in Hermann von Helmholtz, *Popular Scientific Lectures*, edited by Morris Kline, Dover, NY, 1962.
21. Thomas Hobbes, *Leviathan, or the Matter, Form, and Power of a Commonwealth, Ecclesiastical and Civil*, 1651, in E. Burtt, ed., *The English Philosophers from Bacon to Mill*, Modern Library, New York, 1939.
22. Anthony Hyman, *Charles Babbage: Pioneer of the Computer*. Princeton University Press, Princeton, NJ, 1982.
23. Werner Jaeger, *Early Christianity and Greek Paideia*, Oxford University Press, London, Oxford, and New York, 1961.
24. Immanuel Kant, *Critique of Pure Reason*, 1781, tr. F. Max Müller, Macmillan, New York, 1961.
25. ______, *Prolegomena to Any Future Metaphysics*, 1783, ed. Lewis W. Beck, Liberal Arts Press, New York, 1951.
26. Morris Kline, *Mathematics in Western Culture*, Oxford University Press, New York, 1953.

27. D. Landau and P. Lazarsfeld, Quetelet, *International Encyclopedia of the Social Sciences*, Vol. 13, Macmillan, New York, 1968, pp. 247–257.
28. Pierre Simon Laplace, *A Philosophical Essay on Probabilities*, 1819 tr. F. W. Truscott and F. L. Emory, Dover, NY, 1951.
29. Desmond Lee, 1965 Introduction, in Desmond Lee, ed., *Plato: Timaeus and Critias*, Penguin Books of Great Britain, London, 1971.
30. Leibniz, *Preface to the General Science* and *Towards a Universal Characteristic*; 1677; reprint, *Selections*, Philip P. Weiner, editor, 1951, pp. 12–17, 17–25.
31. Thomas R. Malthus, An Essay on the Principle of Population, as it Affects the Future Improvement of Society: with Remarks on the Speculations of Mr. Godwin, M. Condorcet, and other writers, 1798, in Garrett Hardin, ed., *Population, Evolution and Birth Control*, Freeman, San Francisco, 1964, pp. 4–16.
32. Maurice Mandelbaum, The Search for a Science of Society: From Saint-Simon to Marx and Engels, Chapter 4 in Maurice Mandelbaum, *History, Man, and Reason*, Johns Hopkins University Press, Baltimore and London, 1971, pp. 63–76.
33. James Clerk Maxwell, *Theory of Heat*, Longmans, Green, & Co., London, 1871.
34. Seyyed Hossein Nasr, *Science and Civilization in Islam*, New American Library, New York, Toronto and London, 1968.
35. Isaac Newton, Letter to Henry Oldenburg, July, 1672, in [38].
36. ______, Letter to Richard Bentley, December 10, 1692, in [38].
37. ______, *Sir Isaac Newton's Mathematical Principles of Natural Philosophy and His System of the World*, tr. Andrew Motte, revised and edited by Florian Cajori, University of California Press, Berkeley, 1934.
38. ______, *Newton's Philodophy of Nature: Selections from His Writings*, ed. H. S. Thayer, Hafner, New York, 1951.
39. Blaise Pascal, Pensées, E. P. Dutton, New York, 1958.
40. Benjamin Peirce, Linear Associative Algebra, *Amer. J. Math.*, 4 (1881).
41. Plato, *Republic*, tr. A. D. Lindsay, E. P. Dutton, New York, 1950.
42. Plato, Timaeus, in [29].
43. Richard H. Popkin, *The History of Scepticism from Erasmus to Spinoza*, University of California Press, Berkeley and Los Angeles, 1979.
44. Theodore M. Porter, A Statistical Survey of Gases: Maxwell's Social Physics, *Historical Studies in the Physical Sciences* 12 (1981), 77–116.
45. A. Quetelet, *Instructions populaires sur le calcul des probabilités*, Tarlier, Brussels, 1828.
46. Bertrand Russell, *A Critical Exposition of the Philosophy of Leibniz*, 2d edition, Allen and Unwin, London, 1937.
47. William G. Sinnigen and Arthur E. R. Boak, *A History of Rome to A.D. 565*, sixth edition, Macmillan, New York, 1977.
48. Andrew Skinner, Introduction, Adam Smith, *The Wealth of Nations*, (1776), Penguin Books, London, 1974, pp. 11–97.
49. Benedict de Spinoza, *Ethics*, preceded by *On the Improvement of the Understanding*, ed. James Gutmann, Hafner, New York, 1953.
50. François-Marie Arouet de Voltaire, *The Portable Voltaire*, The Viking Press, New York, 1949, selections from *Dictionnaire Philosophique* (1764), pp. 53–228.
51. Joseph Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation*, Freeman, San Francisco, 1976.
52. Harry Austryn Wolfson, What is New in Philo?, in Harry A. Wolfson, *From Philo to Spinoza: Two Studies in Religious Philosophy*, Behrman House, New York, 1977.

Some of the greatest advances in mathematics have been due to the invention of symbols, which it afterwards became necessary to explain; from the minus sign proceeded the whole theory of negative quantities.

Aldous Huxley, *Jesting Pilate*,
London, Chatto and Windus, 1926

NOTES

Kepler's Spheres and Rubik's Cube

JAMES G. PROPP
University of Maryland
College Park, MD 20742

"How many spheres of radius r may simultaneously be tangent to a fixed sphere of the same radius?" This question goes back at least to the year 1694, when it was considered by Isaac Newton and his contemporary David Gregory. Johann Kepler had already shown in 1611 [**8**] that twelve outer spheres could be arranged around a central sphere, and now Gregory claimed that a thirteenth could be added. Newton disagreed, but neither man proved his claim, and it was not until 1874 that a proof was found, substantiating Newton's conjecture. (R. Hoppe's original proof is described in [**2**]; more recently, proofs have been found by Günter [**7**] and by Schütte and van der Waerden [**10**]. Perhaps the most elegant proof known is the one given by John Leech [**9**]. For a history of the problem, see [**6**].)

It's worth noting that the 4-dimensional version of this problem is still unsolved; no one knows how to arrange more than twenty-four hyperspheres around a central hypersphere, but neither has it been shown that a twenty-fifth cannot be added. In higher dimensions the situation is even less well understood, with the remarkable exception of dimensions 8 and 24, for which the maximum contact numbers are precisely known [**1**].

The source of difficulty in the original Gregory-Newton problem (and the reason it took 180 years to be solved) is that there is almost room for a thirteenth sphere; the twelve spheres of Kepler can be pushed and pulled in all sorts of ways, and it's credible that some sort of fiddling could create a space big enough to accommodate an extra sphere.

This note will deal with a related question, in the spirit of Ernö Rubik: **if we label the twelve spheres and roll them over the surface of the inner sphere at will, what permutations are achievable?** The answer is surprising, and the proof requires only the rudiments of analytic geometry and group theory. One fringe benefit of this enterprise is that it leads to a natural coordinatization of the vertices of the regular icosahedron.

An equivalent formulation of the problem is gotten by considering only the centers of the spheres: we imagine twelve vertices, free to move on a sphere of fixed radius $R = 2r$ about a fixed origin but subject to the constraint that no two vertices may ever be closer together than R. We will find it convenient to switch back and forth between the two formulations. For definiteness, put $r = \frac{1}{2}$, $R = 1$.

To begin, we must prescribe an initial configuration for the outer spheres. One possibility that springs to mind is to arrange the twelve vertices to form a regular icosahedron. As we'll see, any two distinct vertices of the icosahedron inscribed in the unit sphere are at least

$$\sqrt{2 - 2/\sqrt{5}} \approx 1.01$$

units apart, so not only is this configuration possible, but no two of the outer spheres touch (see FIGURE 1). It is clear that any rigid motion of the icosahedron about its center can be achieved by a joint motion of the spheres; and so, since the rotational symmetries of the icosahedron comprise the alternating group A_5 [5, pp. 49–50], the number of icosahedral arrangements of the spheres accessible from this starting configuration is at least $|A_5| = 60$.

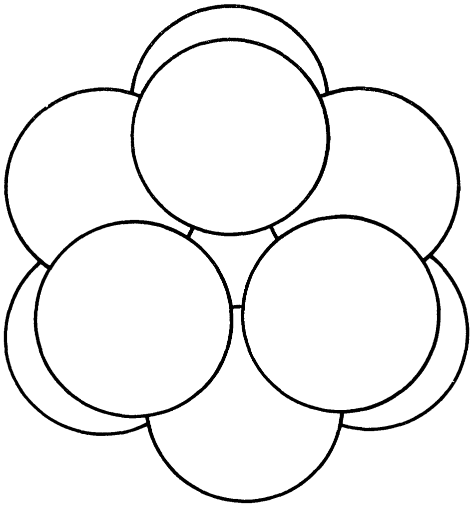


FIGURE 1

But there is another way of placing the twelve spheres around one, and moreover, this arrangement extends to a sphere-packing of three-space. Let the lattice Λ consist of all points $(a/\sqrt{2}, b/\sqrt{2}, c/\sqrt{2})$ with a, b, c integers and $a+b+c$ even. Then no two points of Λ are closer than 1, and so the points of Λ may serve as the centers of non-overlapping spheres of radius $\frac{1}{2}$ (see FIGURE 2). This is the *cubic close-packing* discovered by Kepler. Each vertex has twelve nearest neighbors, and in particular the

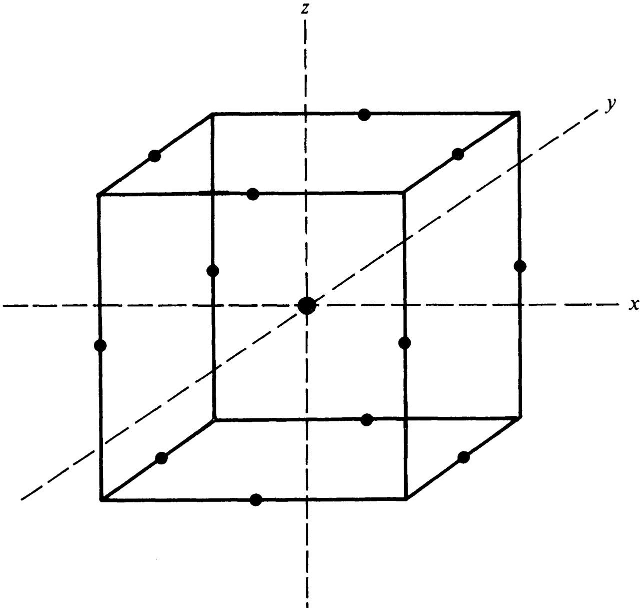


FIGURE 2

neighbors of $(0,0,0)$ are

$$(\pm 1/\sqrt{2}, \pm 1/\sqrt{2}, 0)$$
$$(\pm 1/\sqrt{2}, 0, \pm 1/\sqrt{2})$$
$$(0, \pm 1/\sqrt{2}, \pm 1/\sqrt{2}).$$

These vertices form a *cuboctahedron* (see FIGURE 3(a)). Its rotational symmetry group, like that of the cube and the octahedron, is S_4; one may concretely picture the S_4 action as permuting the four pairs of antipodal triangular faces. Hence at least $|S_4| = 24$ cuboctahedral arrangements are accessible from the initial position. The S_4 action on the vertices, like the A_5 action, performs only even permutations on the twelve vertices/spheres.

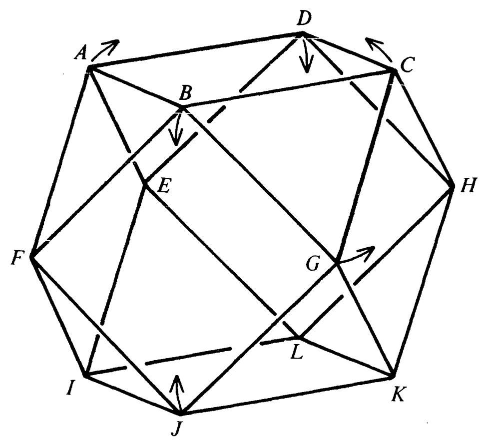


FIGURE 3(a)

Now comes a pleasant surprise: the two arrangements of the twelve spheres (icosahedral and cuboctahedral) may be deformed into one another! This means that in our Rubik-like manipulations, we can avail ourselves of both the A_5 and S_4 symmetries.

To deform the cuboctahedron into the icosahedron, move each point along a great circle (as indicated in FIGURE 3(a) for selected points) so that each square face of the cuboctahedron becomes a pair of triangular faces of the icosahedron. For instance, the points

$$A = \left(-\sqrt{\tfrac{1}{2}}, 0, \sqrt{\tfrac{1}{2}}\right)$$

and

$$C = \left(\sqrt{\tfrac{1}{2}}, 0, \sqrt{\tfrac{1}{2}}\right)$$

both move toward $(0,0,1)$, while the point

$$B = \left(0, -\sqrt{\tfrac{1}{2}}, \sqrt{\tfrac{1}{2}}\right)$$

moves toward $(0, -1, 0)$. (This is a variation on the construction given in [**5**, pp. 51–53].) We may parametrize this joint motion with a variable t, whose initial value is $\pi/4$:

$$A(t) = (-\cos t, 0, \sin t)$$
$$B(t) = (0, -\sin t, \cos t)$$
$$C(t) = (\cos t, 0, \sin t)$$

and so on. The distance between $A(t)$ and $B(t)$ is

$$\sqrt{\cos^2 t + \sin^2 t + (\sin t - \cos t)^2} = \sqrt{2 - \sin 2t}\,,$$

which increases from 1 to $\sqrt{2}$ as t runs from $\pi/4$ to $\pi/2$. The distance between $A(t)$ and $C(t)$ is

$$2\cos t,$$

which decreases from $\sqrt{2}$ to 0 as t approaches $\pi/2$. Let us intervene and stop the process when the lengths of AB and AC are equal, which occurs at some unique time $t = \theta$, and write $A' = A(\theta)$, $B' = B(\theta)$, etc. The symmetry of the procedure now guarantees that $B'C' = A'B' = B'F' = F'A'$, so that triangles $A'B'C'$ and $A'B'F'$ are congruent equilateral triangles. In fact, the vertices $A', \dots, L'$ form twenty such triangles on the sphere of radius R, and this implies that they are arranged icosahedrally, with labelings as shown in FIGURE 3(b).

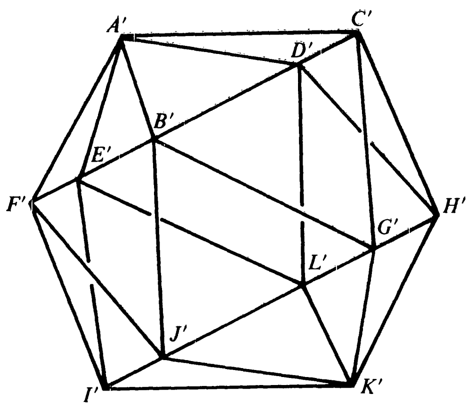


FIGURE 3(b)

(By equating

$$(A'B')^2 = 2 - \sin 2\theta$$

and

$$(A'C')^2 = 4\cos^2\theta = 2 + 2\cos 2\theta$$

one obtains

$$\cos 2\theta = \frac{-1}{\sqrt{5}} \text{ and } \sin 2\theta = \frac{2}{\sqrt{5}}\,,$$

so that the common length of the segments is

$$\sqrt{2 - 2/\sqrt{5}}\,.$$

This is the side-length of an icosahedron of circumradius 1. Also, the distance between A' and I' is $2\sin\theta$, whose ratio to $A'C' = A'B' = 2\cos\theta$ is $\tan\theta$; this may easily be shown to equal the golden ratio $(1+\sqrt{5})/2$. Hence $A'I'K'C'$ is a golden rectangle, as is any rectangle formed by two diagonals of the icosahedron.)

Since it does not matter whether our initial configuration is icosahedral or cuboctahedral, we may as well assume the latter. Let G be the group of permutations of the twelve spheres that can be achieved by the operations of rotating the cuboctahedron, switching between cuboctahedral and icosahedral formation, and rotating the icosahedron, in all combinations. (We don't claim that G contains *all* the achievable permutations.) Note that points which were antipodal at the start remain antipodal throughout. Also note that since G contains copies of both S_4 and A_5, its order is at least 120.

If we rotate the labeled icosahedron of FIGURE 3(b) by 72 degrees clockwise about its axis $A'K'$, the points are permuted by

$$(A')(B'C'D'E'F')(G'H'L'I'J')(K')$$

which corresponds to the permutation

$$\gamma=(A)(BCDEF)(GHLIJ)(K)$$

of the vertices of the cuboctahedron. On the other hand, if we rotate the cuboctahedron by 90 degrees clockwise about the vertical axis, the points are permuted by

$$\alpha=(ABCD)(EFGH)(IJKL).$$

Since each of these permutations belongs to G, so does their product

$$\alpha\gamma=(ABDFC)(EG)(HIKLJ).$$

But $(\alpha\gamma)^5=$ the two-cycle (EG). Hence, in general, any two antipodal points may be exchanged without affecting the final position of the other ten.

The preceding observation tells us that the group G is a wreath product of the form $2^6.H$, where H is a group acting on *pairs* of antipodal points. (For an explanation of this notation, see [3].) That is, every element of G is uniquely determined by its action on the six principal diagonals of the polyhedron, with a choice of orientation; if you like, think of H as a permutation group acting on six coins, and $2^6.H$ as the set of actions one gets by allowing not only permutations taken from H but also arbitrary flips. Let $\bar{A}$, $\bar{B}$, etc., denote the diagonals AK, BL, etc. Then the image of γ under the natural homomorphism from G to H is

$$\bar{\gamma}=(\bar{A})(\bar{B}\bar{C}\bar{D}\bar{E}\bar{F}),$$

and similarly, the image of α is

$$\bar{\alpha}=(\bar{A}\bar{B}\bar{C}\bar{D})(\bar{E}\bar{F}).$$

To find generators of the group H, we need to know the generators of G. α and γ aren't enough, but we'll only need one more. The S_4 subgroup of G is generated by

$$\alpha=(ABCD)(EFGH)(IJKL)$$

(90 degree rotation about the axis through face $ABCD$) and

$$\beta=(ABF)(CJE)(DGI)(HKL)$$

(120 degree rotation about the axis through face ABF), while the A_5 subgroup is generated by

$$\gamma=(A)(BCDEF)(GHLIJ)(K)$$

(72 degree rotation about axis $A'K'$) and

$$\delta=(ABF)(CJE)(DGI)(HKL)=\beta$$

(120 degree rotation about the axis through face $A'B'F'$). The images of those elements in H are

$$\bar{\alpha}=(\bar{A}\,\bar{B}\,\bar{C}\,\bar{D})(\bar{E}\,\bar{F})$$
$$\bar{\beta}=(\bar{A}\,\bar{B}\,\bar{F})(\bar{C}\,\bar{D}\,\bar{E})$$
$$\bar{\gamma}=(\bar{A})(\bar{B}\,\bar{C}\,\bar{D}\,\bar{E}\,\bar{F})$$

and they must generate H.

Since all three permutations are even, H must be a subgroup of the alternating group A_6, and in fact H is A_6 itself. We prove this by successively examining stabilizer subgroups:

1. The action of H on $\bar{A}, \bar{B}, \bar{C}, \bar{D}, \bar{E}, \bar{F}$ is clearly transitive, so all of its 1-point stabilizer subgroups are isomorphic, and have order $|H|/6$.

2. $\bar{\gamma}$ (which belongs to the stabilizer of $\bar{A}$) acts transitively on $\bar{B}, \bar{C}, \bar{D}, \bar{E}, \bar{F}$, so that all 2-point stabilizer subgroups are isomorphic, and have order $|H|/6\cdot 5$.

3. Since

$$\bar{\alpha}^2=(\bar{A}\,\bar{C})(\bar{B}\,\bar{D})(\bar{E})(\bar{F})$$

and

$$\bar{\beta}\bar{\alpha}\bar{\beta}=(\bar{A}\,\bar{D})(\bar{B}\,\bar{C})(\bar{E})(\bar{F})$$

(which belong to the stabilizer of $\bar{E}, \bar{F}$) generate a transitive action on $\bar{A}, \bar{B}, \bar{C}, \bar{D}$, all the 3-point stabilizer subgroups of H are isomorphic, and have order $|H|/6\cdot 5\cdot 4$.

4. But since

$$\bar{\alpha}\bar{\gamma}^{-1}=(\bar{A}\,\bar{B}\,\bar{E})(\bar{C})(\bar{D})(\bar{F})$$

belongs to the stabilizer of $\bar{C}, \bar{D}, \bar{F}$, this 3-point stabilizer must contain the cyclic group A_3. In fact, it must be A_3 itself (S_3 is impossible, since $\bar{\alpha}, \bar{\beta}, \bar{\gamma}$ are all even). Hence $|H|/6\cdot 5\cdot 4=3$, so that $|H|=360$ and $H=A_6$, as claimed.

We have now shown that the S_4 and A_5 symmetry groups (of the cuboctahedron and icosahedron, respectively) combine to give a group $G=2^6.A_6$ of order $2^6\cdot(6!/2)=23{,}040$. But might there be even more feasible permutations of the twelve spheres?

Here's an idea, inspired by the twisting operation one performs on a Rubik's cube. Perhaps one can pull six of the spheres tightly to one side (or "hemisphere") of the central sphere, and six to the other side, in such a way that the two groups can be twisted past one another. Specifically, we arrange two of the twelve spheres antipodally, and around each we cluster five spheres as snugly as possible, forming two "caps" (top view shown in FIGURE 4(a)). The question is, can the caps be twisted past each other?

This is equivalent to asking whether the sphere in the middle of such a cap (at the "north pole", as it were) can simultaneously touch all five surrounding spheres. For, if such perfectly snug caps are possible, then six spheres can be restricted to the northern hemisphere, and the five that border on the "equator" will graze but not block the other six spheres, which are all restricted to the southern hemisphere (see FIGURE 4(b)). So now we need only check whether five points, all with latitude 30 degrees North on a sphere of radius $R = 1$, can all be at least distance 1 from each other. (Or equivalently: Can five non-overlapping regular tetrahedra share an edge? To see the connection, let the common edge be the segment joining the origin to the north pole.)

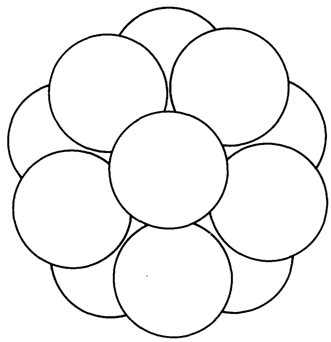


FIGURE 4(a)

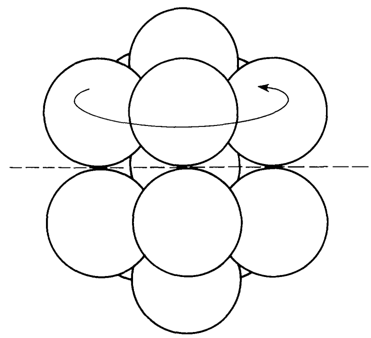


FIGURE 4(b)

But this is simple trigonometry: A regular pentagon inscribed in a circle of radius 1 has side

$$\sqrt{2 - 2\cos\frac{2\pi}{5}} = \sqrt{\frac{5-\sqrt{5}}{2}},$$

so one inscribed in a latitude circle of radius $\sqrt{3}/2$ has side

$$\sqrt{\frac{5-\sqrt{5}}{2}}\,\frac{\sqrt{3}}{2} \approx 1.02.$$

This is just barely bigger than 1, but it's enough to ensure that the caps can indeed be made snug and then twisted past each other.

The "twisting" move we have described is a 5-cycle that may be performed on any 5 vertices of the icosahedron that form a regular pentagon. Since such permutations are even, the group they generate must lie in A_{12}. To see what this group is, consider the situation shown in FIGURE 5(a), with two pentagons intersecting in two points. Let

$$\alpha = (ABGHD)$$

and

$$\beta = (BFIKG).$$

Then

$$\alpha^{-1}\beta^{-1}\alpha\beta = (AB)(GK).$$

By conjugating this permutation through elements of the 2-point stabilizer of A, B, one may show that every permutation $(AB)(XY)$ (with $X, Y \neq A, B$) can be achieved. (Look at FIGURE 5(b). Take a pencil and mark those edges to which edge GK can be moved by rotating a pentagon that doesn't contain A or B; it will be seen that all edges XY not involving A and B eventually get marked, and the moves that

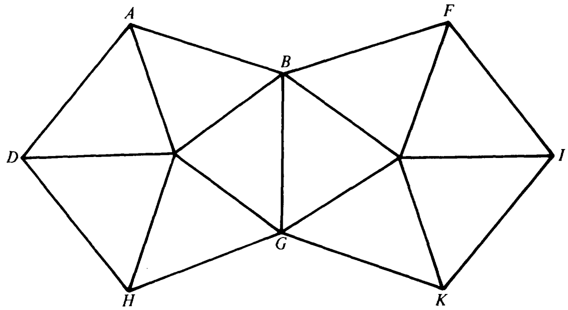


FIGURE 5(a)

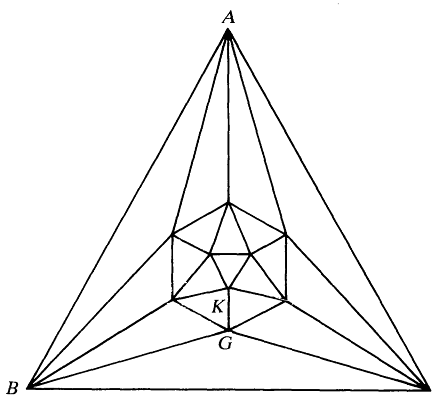


FIGURE 5(b)

carry edge GK to the respective edges XY give precisely the conjugations we need to obtain all permutations of the form $(AB)(XY)$.) The same sort of argument now shows that in fact any permutation of the shape $(VW)(XY)$ can be achieved. Since A_{12} is simple, the normal subgroup generated by these pairs of transpositions must be A_{12} itself. Hence, the twisting moves allow any even permutation on the twelve spheres to be performed.

What happens if we now allow both the cuboctahedron-to-icosahedron maneuver and the twist operation? Recall that the group $G = 2^6H$ contains two-cycles that exchange antipodes. Even one such two cycle, if adjoined to the group A_{12}, suffices to generate the full symmetric group S_{12}. (Alternatively, one can regard G as primary, and adjoin to it a few 5-cycles so that every pair of spheres can be made antipodal; for we already know how to exchange antipodes at will.) In either case, we see that *every* permutation of the twelve spheres is feasible, and the "Rubik group" of Kepler's spheres is S_{12}.

Some concluding remarks:

1. It may interest the reader to know that a related problem leads not to S_{12} but to the Mathieu group M_{12}, one of the sporadic finite simple groups; see [4].

2. There are many more possible arrangements of the twelve spheres than the cuboctahedral and icosahedral formations, yet the theorem proved above says nothing about twelve-spheres-around-one in general position. It seems likely that every position can be reached from every other; to prove this, it would suffice to show that every configuration can be "tidied" into icosahedral formation. Perhaps some reader will be able to find a proof.

3. If anyone built a working model of "Kepler's Spheres," he or she would probably give the outer spheres slightly smaller radius than the inner sphere to prevent jamming, since both the icosahedron-to-cuboctahedron maneuver and the twist operation cause spheres to graze one another. This suggests the following question: if the outer spheres in an icosahedral arrangement were given slightly *larger* radius than the inner sphere, would any permutations be possible aside from the "trivial" ones obtained from A_5? Perhaps engineers have already developed a theory for handling such problems of constrained motion in space—if so, the author would be glad to hear of it.

The problem addressed in this paper and the solution given here were developed jointly by Eugenio Calabi, John Conway and myself during Conway's lectures on "Games, Groups, Lattices, and Loops" at the University of Pennsylvania. During the writing of this article, I was supported by a National Science Foundation Graduate Fellowship.

REFERENCES

1. E. Bannai and N. J. A. Sloane, Uniqueness of certain spherical codes, *Canad. J. Math.* 33 (1981), 437–449.
2. C. Bender, Bestimmung der grössten Anzahl gleich grosser Kugeln, welche sich auf eine Kugel von demselben Radius, wie die übrigen, auflegen lassen, *Grunert Arch.* 56 (1874), 302–313.
3. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *An Atlas of Finite Groups*, Clarendon Press, 1985.
4. J. H. Conway and N. J. A. Sloane, *The Leech Lattice, Sphere Packings, and Related Topics*, to appear.
5. H. S. M. Coxeter, *Regular Polytopes*, Dover, 3rd ed., 1973.
6. H. S. M. Coxeter, *Twelve Geometric Essays*, Southern Illinois Univ. Press, 1968, pp. 179–198.
7. S. Günter, Ein Stereometrisches Problem, *Grunert Arch.* 57 (1875), 209–215.
8. J. Kepler, *The Six-Cornered Snowflake*, Oxford Univ. Press, 1966.
9. John Leech, The problem of the thirteen spheres, *Math. Gaz.* 40 (1956), 22–23.
10. K. Schütte and B. L. van der Waerden, Das Problem der dreizehn Kugeln, *Math. Ann.* 125 (1953), 325–334.

A Characterization of Infinite Dimension for Vector Spaces

HENRY HEATHERLY
University of Southwestern Louisiana
Lafayette, LA 70504

Several different arguments have been used to establish that a finite-dimensional vector space over the real or complex number fields cannot have a pair of linear transformations whose commutator is the identity; i.e., $[A, B] = AB - BA = 1$ is impossible for such spaces. The oldest argument is implicit in the comments of Max Born and Pacual Jordan in their seminal work on a matrix version of quantum mechanics [1]. They noted that for finite matrices (over the complex numbers), applying the trace function to the equation

$$PQ - QP = \frac{h}{2\pi i}1$$

3. If anyone built a working model of "Kepler's Spheres," he or she would probably give the outer spheres slightly smaller radius than the inner sphere to prevent jamming, since both the icosahedron-to-cuboctahedron maneuver and the twist operation cause spheres to graze one another. This suggests the following question: if the outer spheres in an icosahedral arrangement were given slightly *larger* radius than the inner sphere, would any permutations be possible aside from the "trivial" ones obtained from A_5? Perhaps engineers have already developed a theory for handling such problems of constrained motion in space—if so, the author would be glad to hear of it.

The problem addressed in this paper and the solution given here were developed jointly by Eugenio Calabi, John Conway and myself during Conway's lectures on "Games, Groups, Lattices, and Loops" at the University of Pennsylvania. During the writing of this article, I was supported by a National Science Foundation Graduate Fellowship.

REFERENCES

1. E. Bannai and N. J. A. Sloane, Uniqueness of certain spherical codes, *Canad. J. Math.* 33 (1981), 437–449.
2. C. Bender, Bestimmung der grössten Anzahl gleich grosser Kugeln, welche sich auf eine Kugel von demselben Radius, wie die übrigen, auflegen lassen, *Grunert Arch.* 56 (1874), 302–313.
3. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *An Atlas of Finite Groups*, Clarendon Press, 1985.
4. J. H. Conway and N. J. A. Sloane, *The Leech Lattice, Sphere Packings, and Related Topics*, to appear.
5. H. S. M. Coxeter, *Regular Polytopes*, Dover, 3rd ed., 1973.
6. H. S. M. Coxeter, *Twelve Geometric Essays*, Southern Illinois Univ. Press, 1968, pp. 179–198.
7. S. Günter, Ein Stereometrisches Problem, *Grunert Arch.* 57 (1875), 209–215.
8. J. Kepler, *The Six-Cornered Snowflake*, Oxford Univ. Press, 1966.
9. John Leech, The problem of the thirteen spheres, *Math. Gaz.* 40 (1956), 22–23.
10. K. Schütte and B. L. van der Waerden, Das Problem der dreizehn Kugeln, *Math. Ann.* 125 (1953), 325–334.

A Characterization of Infinite Dimension for Vector Spaces

HENRY HEATHERLY
University of Southwestern Louisiana
Lafayette, LA 70504

Several different arguments have been used to establish that a finite-dimensional vector space over the real or complex number fields cannot have a pair of linear transformations whose commutator is the identity; i.e., $[A, B] = AB - BA = 1$ is impossible for such spaces. The oldest argument is implicit in the comments of Max Born and Pacual Jordan in their seminal work on a matrix version of quantum mechanics [**1**]. They noted that for finite matrices (over the complex numbers), applying the trace function to the equation

$$PQ - QP = \frac{h}{2\pi i}1$$

leads to zero on the left and not zero on the right. From this they concluded that this basic equation, the "sharpened quantum condition," had to be in terms of infinite matrices. It is unlikely that Born and Jordan were the first to make use of this observation concerning trace and commutators, for while they were more knowledgeable about matrix algebra than most physicists of that time (1925), neither was an expert in the theory. (For more on the role matrix theory played in physics before and during the great age of quantum mechanics, see the excellent account by Mehra and Rechenberg [3].)

The Trace Argument

Let V be a finite-dimensional vector space over a field K of characteristic zero. If α and β are linear transformations on V such that $[\alpha, \beta] = 1$, then the assumption that $\dim_K V = N < \infty$, leads to a pair of n by n matrices over K, say, A and B, such that $[A, B] = I$. Since trace AB = trace BA, this leads to $0 = \text{trace}[A, B] = \text{trace } I = n \cdot 1$.

This last equation suggests something different might happen if K has prime characteristic, which is indeed the case. (See [2].)

In the subsequent development of quantum mechanics, calculations concerning quantum mechanical matrices P, Q for various physical systems (e.g., the linear oscillator, the hydrogen atom) showed these infinite matrices could not be bounded operators on Hilbert's space. A rigorous general proof of this was not given until 1947 (Aurel Wintner [7]). Wintner's proof is specialized and makes use of technical properties of the spectrum of the operators. Not long after Wintner's paper appeared, Helmut Wielandt gave an elementary, albeit abstract, proof of the result—and much more [6].

Wielandt's Argument

The setting is that of a normed, linear associative algebra [4]. This is a normed vector space (over the real or complex number fields), with a multiplication defined on the vectors so the resulting system is a ring with unity and such that for any vectors x, y and scalar λ:

$$\text{(i)} \quad (\lambda x)y = x(\lambda y) = \lambda(xy);$$

$$\text{(ii)} \quad \|xy\| \leqslant \|x\| \cdot \|y\|.$$

Let W be such an algebra. Suppose $a, b \in W$ such that $[a, b] = ab - ba = 1$. By induction on n one establishes

$$a^{n+1}b - ba^{n+1} = (n+1)a^n, \qquad n = 0, 1, 2, \dots .$$

Note that $a \neq 0$. If a is nilpotent, then $a^m = 0$ for some minimal $m \geqslant 2$. This leads to

$$0 = a^m b - ba^m = (m-1)a^{m-1} \quad \text{or} \quad a^{m-1} = 0.$$

Consequently, $a^n \neq 0$ and $\|a^n\| \neq 0$ for each n. Then

$$\|(n+1)a^n\| = \|a^{n+1}b - ba^{n+1}\| \leqslant \|a^{n+1}\| \cdot \|b\| + \|b\| \cdot \|a^{n+1}\|,$$

or

$$(n+1)\|a^n\| \leqslant 2\|a^n\| \cdot \|a\| \cdot \|b\|$$

and, hence,

$$(n+1) \leqslant 2\|a\| \cdot \|b\|,$$

for all n. Thus a normed linear algebra cannot contain such a pair of elements.

The bounded linear transformations on a normed vector space form a normed algebra. (Use $\|T\| = \sup\|Tx\|$, where $\|x\| \leqslant 1$, [5, pp. 162–163].) So the equation $[A, B] = 1$ is impossible for bounded linear transformations. Wintner's result for quantum mechanical matrices follows immediately.

Any finite-dimensional vector space over the real or complex numbers can be made into a normed space and all the linear transformations on the space are bounded. So if a vector space (over the real or complex numbers) has a pair of linear transformations satisfying $[A, B] = 1$, then the space must be infinite dimensional.

Each of the two arguments given has appeal, but each makes use of an extrinsic idea: trace or norm. Neither of the concepts is necessary.

The Linear Independence Argument

Let V be a vector space over a field of characteristic zero. If A, B are linear transformations on V such that $[A, B] = 1$, then

$$A^{n+1}B - BA^{n+1} = (n+1)A^n,$$

for $n = 0, 1, 2, \dots$. Use this identity and mathematical induction to establish that the set $1, A, A^2, \dots$ is linearly independent. Then the space of all linear transformations on V is not finite dimensional and consequently V is not finite dimensional.

Each of these three arguments does not hold if the field of scalars has prime characteristic. In fact, the result is not true in that case. If the characteristic of the field is p and the space has dimension divisible by p, then such a pair of transformations exists [2].

Existence on Infinite-Dimensional Spaces

A concrete example shows linear transformations having the desired property do exist. The example also hints at how to prove existence of such pairs on any infinite-dimensional space. Let P be the space of all polynomial forms over a field K and let D and $x1$ be the operators defined by: $Df(x) = f'(x)$ and $x1f(x) = xf(x)$, for all $f(x) \in P$. Note that $D \cdot (x1) - (x1) \cdot D = 1$. The hint on how to build the desired pairs in general comes from looking at the action of D and $x1$ on the basis $1, x, x^2, \dots$:

$$D1 = 0, \qquad Dx^n = nx^{n-1}, \qquad n = 1, 2, \dots;$$
$$x1x^n = x^{n+1}, \qquad n = 0, 1, 2, \dots.$$

Let V be an infinite-dimensional vector space. Select a basis for V and write it as the disjoint union of the subsets

$$B_j = \{b_{jn}\colon n = 0, 1, 2, \dots\},$$

where j is from an arbitrary index set so that $\cup B_j$ is a basis for V. Define the functions α and β on the basis via:

$$\alpha b_{j0} = 0, \qquad \alpha b_{jn} = n b_{j,n-1}, \qquad n = 1, 2, \ldots;$$
$$\beta b_{jn} = b_{j,n+1}, \qquad n = 0, 1, 2, \ldots.$$

Then $(\alpha\beta - \beta\alpha)b_{jn} = b_{jn}$, for each j, n. Extend α and β to linear transformations α' and β' (respectively) and note that $[\alpha', \beta'] = 1_V$.

Putting all the pieces together we have:

THEOREM. *Let V be a vector space over a field of characteristic zero. The following are equivalent*:

(i) *V is infinite dimensional;*

(ii) *there exist linear transformations A, B on V such that* $[A, B] = 1_V$.

The existence proof shows how to build large numbers of such pairs. If $[A, B] = 1_V$, then for any invertible T on V,

$$[TAT^{-1}, TBT^{-1}] = 1_V.$$

An interesting problem is to classify all pairs whose commutator is the identity. The existence of pairs of endomorphisms on modules with the property $[A, B] = 1$ is discussed in [2]. In general, the question is an open one.

The author would like to acknowledge the helpfulness of conversations and correspondence with Professor P. R. Halmos.

REFERENCES

1. M. Born and P. Jordan, Zur Quantenmechanik, Z. *Phys.* 34 (1925), 858–888.
2. H. Heatherly, *Matrices, morphisms, and algebras with* $[A, B] = 1$, to appear.
3. J. Mehra and H. Rechenberg, *The Historical Development of Quantum Theory*, vol. 3, *The Formulation of Matrix Mechanics and its Modifications 1925–1926*, Springer-Verlag, New York, 1982.
4. C. Rickart, *General Theory of Banach Algebras*, Robert E. Krieger, Huntington, 1974.
5. A. Taylor, *Introduction to Functional Analysis*, John Wiley & Sons, New York, 1963.
6. H. Wielandt, Über die Unbeschränktheit der Schrödingerschen der Quantenmechanik, *Math. Ann.* 121 (1949), 21.
7. A. Wintner, The unboundedness of quantum-mechanical matrices, *Phys. Rev.* 71 (1947), 738–739.

Illustrating Hypothesis Testing Concepts: the Student's *t*- vs the Sign Test

LEROY A. FRANKLIN
University of Central Florida
Orlando, FL 32816

While most students have been introduced to concepts such as power of a test, assumptions underlying a test, and what it means to be able/unable to reject the null hypothesis in their first course in statistics, many simply do not have a very strong grasp of these concepts or their importance. It has been the author's experience that the following examples, presented near the end of the first course in statistics, not only

$$\alpha b_{j0} = 0, \qquad \alpha b_{jn} = n b_{j,n-1}, \qquad n = 1,2,\dots;$$
$$\beta b_{jn} = b_{j,n+1}, \qquad n = 0,1,2,\dots.$$

Then $(\alpha\beta - \beta\alpha)b_{jn} = b_{jn}$, for each j, n. Extend α and β to linear transformations α' and β' (respectively) and note that $[\alpha', \beta'] = 1_V$.

Putting all the pieces together we have:

THEOREM. *Let V be a vector space over a field of characteristic zero. The following are equivalent*:

(i) *V is infinite dimensional*;

(ii) *there exist linear transformations A, B on V such that* $[A, B] = 1_V$.

The existence proof shows how to build large numbers of such pairs. If $[A, B] = 1_V$, then for any invertible T on V,

$$[TAT^{-1}, TBT^{-1}] = 1_V.$$

An interesting problem is to classify all pairs whose commutator is the identity. The existence of pairs of endomorphisms on modules with the property $[A, B] = 1$ is discussed in [2]. In general, the question is an open one.

The author would like to acknowledge the helpfulness of conversations and correspondence with Professor P. R. Halmos.

REFERENCES

1. M. Born and P. Jordan, Zur Quantenmechanik, Z. *Phys.* 34 (1925), 858–888.
2. H. Heatherly, *Matrices, morphisms, and algebras with* $[A, B] = 1$, to appear.
3. J. Mehra and H. Rechenberg, *The Historical Development of Quantum Theory*, vol. 3, *The Formulation of Matrix Mechanics and its Modifications 1925–1926*, Springer-Verlag, New York, 1982.
4. C. Rickart, *General Theory of Banach Algebras*, Robert E. Krieger, Huntington, 1974.
5. A. Taylor, *Introduction to Functional Analysis*, John Wiley & Sons, New York, 1963.
6. H. Wielandt, Über die Unbeschränktheit der Schrödingerschen der Quantenmechanik, *Math. Ann.* 121 (1949), 21.
7. A. Wintner, The unboundedness of quantum-mechanical matrices, *Phys. Rev.* 71 (1947), 738–739.

Illustrating Hypothesis Testing Concepts: the Student's *t*- vs the Sign Test

LEROY A. FRANKLIN
University of Central Florida
Orlando, FL 32816

While most students have been introduced to concepts such as power of a test, assumptions underlying a test, and what it means to be able/unable to reject the null hypothesis in their first course in statistics, many simply do not have a very strong grasp of these concepts or their importance. It has been the author's experience that the following examples, presented near the end of the first course in statistics, not only clarify understanding of these concepts but also go a long way to dispel the notion of "you can prove anything with statistics."

The following discussion involves a one sample test of hypothesis and assumes that the student's *t*-test and the sign test have been introduced. The well-known *t*-test assumes the underlying population is normally distributed and is usually formulated as a test on the mean of the population, μ. However, under the normality assumption (since the normal distribution is symmetric), the *t*-test could also be formulated as a test on the median of the population, Median. The sign test [1] is also well known, being one of the oldest nonparametric procedures, and is a test on the median of the population. But it assumes neither normality nor symmetry. Rather, it only assumes that the underlying population is continuous and is at least ordinal in scale.

Finally the following discussion also assumes that a less well-known test, the Lilliefors Test of Normality [2], has been introduced. To apply the test, a sample is taken from a population and the sample mean, $\bar{x}$, and sample variance, s^2, are computed. The original data are then converted to "standardized scores" by computing $z_i = (x_i - \bar{x})/s$ for each observation, x_i. The cumulative distribution function of these "standardized data" is then drawn on special graph paper that has been created to provide 95% Lilliefors Bounds for various sized samples. Should the cumulative distribution function fall outside the bounds for the particular sample size in question, the investigator concludes the underlying population is nonnormal (with $\alpha = .05$). While few introductory statistics texts introduce either the sign test or Lilliefors test, both are easily presented, intuitively appealing, and easily grasped.

Two Examples Where the *t*- and Sign Tests Disagree

The notable feature of this discussion is that with the introduction of both *t*- and sign tests, the student has two different techniques to use to examine a given problem. Most students feel they understand the situation where both tests *agree* to reject the null hypothesis or where both tests agree *not* to reject the null hypothesis. However, the author is convinced that it is precisely when the tests *disagree* that greatest illumination is provided to the students.

The class is given data set 1 (See TABLE 1) as a problem and asked to test H_0: Median = 27 vs H_a: Median < 27 at $\alpha = .05$. Application of the *t*-test gives $\bar{x}_1 = 26$, $s_1 = 1.43$ and a resulting test statistic of 2.42 with observed significance level of .025. Hence, one can *reject* H_0. The class is then given set 1 but asked to test the same hypothesis with the sign test. The observed significance level turns out to be .0729 and, hence, we do not reject H_0! This provides a natural setting to discuss the greater power that the *t*-test has relative to the sign test and the source of that power that lies in the more stringent assumptions of the *t*-test. Also it is appropriate to reiterate that just because "we were unable to reject H_0" does *not* necessarily imply that "H_0 is true." A review of type I and type II errors seems to bring final resolution to the "apparent contradiction."

Immediately the class is given data set 2 (See TABLE 1) and again asked to test H_0: Median = 27 vs H_a: Median < 27 at $\alpha = .05$. Application of the *t*-test gives $\bar{x}_2 = 26$ (the same value as in data set 1), $s_2 = 2.52$ and a resulting test statistic of 1.37 with observed significance level of .10. Hence we can *not* reject H_0! This example then illustrates (thus far) that the sample mean is not the only influential factor in determining the significances of a test, but that the sample variance must also be taken into account. Finally we test data set 2 with the sign test and find the observed

TABLE 1

Data Set 1		Data Set 2	
23.0		23.0	
25.0		24.0	
26.0		24.0	
26.5	$n = 12$	26.0	$n = 12$
25.0		25.0	
26.0	$\bar{x}_1 = 26$	26.0	$\bar{x}_2 = 26$
28.0		31.0	
25.0	$s_1^2 = 2.045$	26.0	$s_2^2 = 6.36$
28.0		25.0	
26.0	$s_1 = 1.430$	31.0	$s_2 = 2.52$
27.5		25.0	
26.0		26.0	

significance level to be .0192 and, hence, we reject H_0! At this point "confusion usually reigns" with students being adamant in insisting "but you told us the t-test was more powerful."

Order is restored by a graphing of the two data sets, something the class is reminded they should always undertake, and a further reminder of the *assumptions* made for each test, most notably the assumption of normality for the t-test (see FIGURES 1 and 2). What the eye suspects in data sets 1 and 2 is confirmed by Lilliefors Tests (see FIGURES 3 and 4). That is, while the data set 1 seems reasonably normal (again caution must be exercised in the interpretation of nonrejection of the null hypothesis of normality), data set 2 is significantly "nonnormal". Thus our tests conducted with the first data set are *appropriate* and the discussion of their power germaine. But since the second data set has been shown to be nonnormal, to apply the t-test to it is not only inappropriate and incorrect, it is also misleading. Of particular note is the role of the two values of 31 in affecting $\bar{x}_2$ and s_2 as "influential observations."

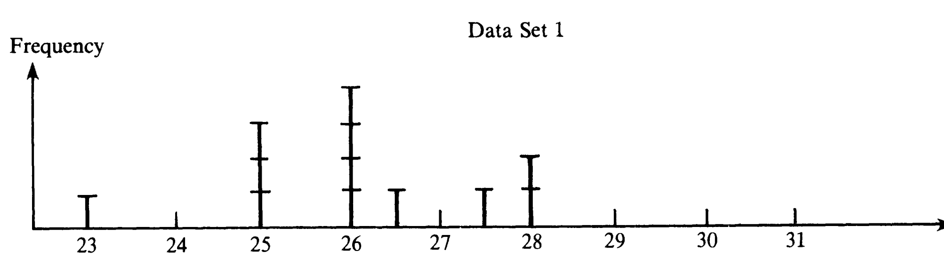


FIGURE 1

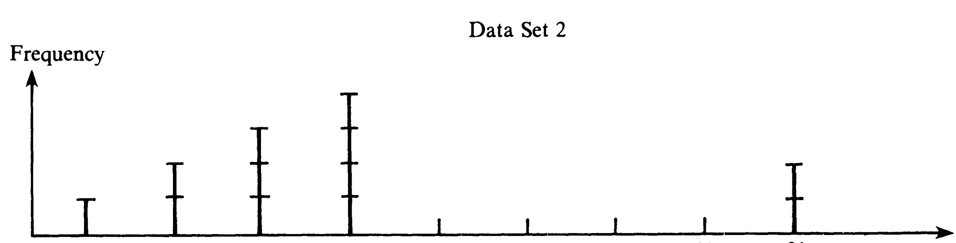


FIGURE 2

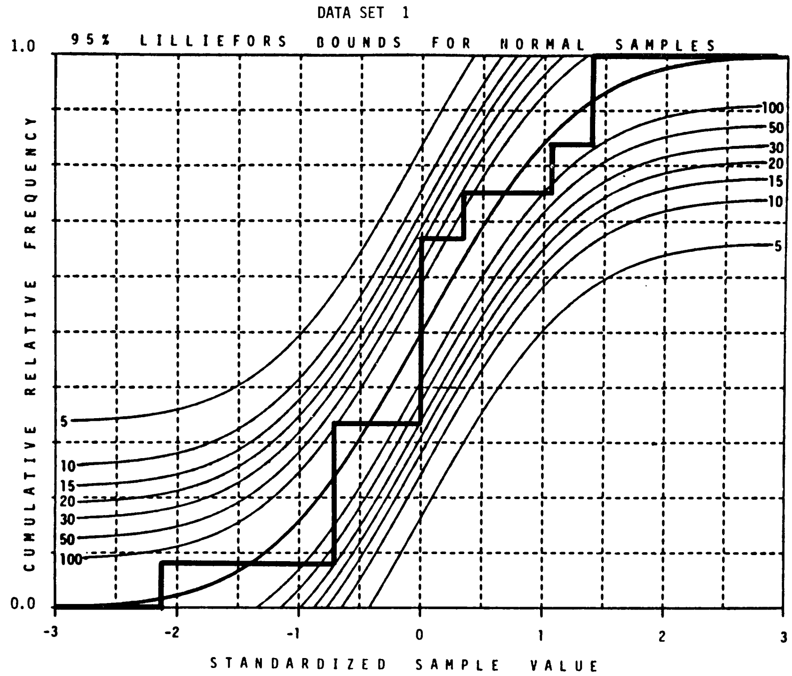


FIGURE 3

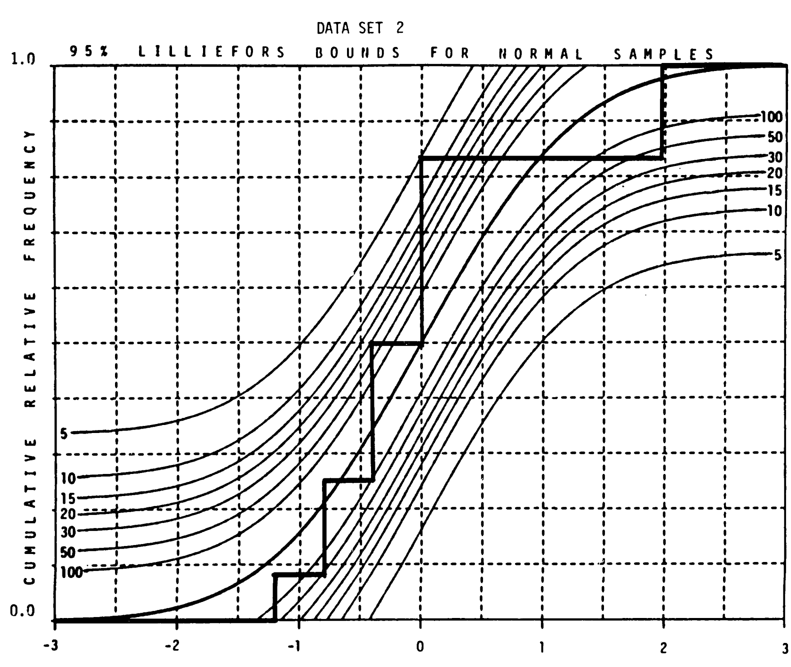


FIGURE 4

Conclusion

The class hour is closed by noting that "seemingly contradictory" statistical results can frequently be resolved by examining the tests run on the data for relative power and for appropriateness (i.e., are the assumptions of the test reasonably satisfied). Hence, many students are disuaded from believing that "you can prove anything with statistics" to endorsing what the author feels is a more enlightened perspective—"it is easy to practice statistics—badly."

REFERENCES

1. Wayne W. Daniel, *Applied Nonparametric Statistics*, Houghton Mifflin Company, Boston, 1978.
2. Ronald L. Iman and W. J. Conover, *A Modern Approach to Statistics*, John Wiley and Sons, New York, 1983.

On Vector Indices mod *m*

I. J. SCHOENBERG
University of Wisconsin-Madison
Madison, WI 53706

1. Introduction

I recently wrote the note [2] on the Chinese Remainder Theorem (abbreviated to C.R.T.), which seems suitable as an elementary introduction to this important topic. The present note was written in 1975 during a one-semester course on number theory at San Diego State University, and provides a suitable sequel to the note mentioned above.

Its purpose is to apply the C.R.T. to obtain the main structural properties of a reduced residue system (abbreviated to R.R.S.) for a modulus m which admits no primitive root, like the modulus $m = 100$. This subject is discussed by W. J. LeVeque in chapter 4, p. 12 of his fine book [1].

Our discussion will be based on two fundamental theorems, the first of which is

THEOREM 1 (The Chinese Remainder Theorem). *Let*

$$m_i(i=1,\dots,n), \qquad m = m_1 m_2 \cdots m_n, \tag{1.1}$$

be n moduli such that

$$(m_i, m_j) = 1 \quad if \quad i \neq j. \tag{1.2}$$

Given the n integers a_i, then there is a unique solution x mod m satisfying the n congruences

$$x \equiv a_i \bmod m_i. \tag{1.3}$$

For proofs and ways of deriving the unknown x, see [2]. The second theorem that we

Conclusion

The class hour is closed by noting that "seemingly contradictory" statistical results can frequently be resolved by examining the tests run on the data for relative power and for appropriateness (i.e., are the assumptions of the test reasonably satisfied). Hence, many students are disuaded from believing that "you can prove anything with statistics" to endorsing what the author feels is a more enlightened perspective—"it is easy to practice statistics—badly."

REFERENCES

1. Wayne W. Daniel, *Applied Nonparametric Statistics*, Houghton Mifflin Company, Boston, 1978.
2. Ronald L. Iman and W. J. Conover, *A Modern Approach to Statistics*, John Wiley and Sons, New York, 1983.

On Vector Indices mod *m*

I. J. SCHOENBERG
University of Wisconsin-Madison
Madison, WI 53706

1. Introduction

I recently wrote the note [2] on the Chinese Remainder Theorem (abbreviated to C.R.T.), which seems suitable as an elementary introduction to this important topic. The present note was written in 1975 during a one-semester course on number theory at San Diego State University, and provides a suitable sequel to the note mentioned above.

Its purpose is to apply the C.R.T. to obtain the main structural properties of a reduced residue system (abbreviated to R.R.S.) for a modulus m which admits no primitive root, like the modulus $m = 100$. This subject is discussed by W. J. LeVeque in chapter 4, p. 12 of his fine book [1].

Our discussion will be based on two fundamental theorems, the first of which is

THEOREM 1 (The Chinese Remainder Theorem). *Let*

$$m_i(i=1,\dots,n), \qquad m = m_1 m_2 \cdots m_n, \tag{1.1}$$

be n moduli such that

$$(m_i, m_j) = 1 \quad if \quad i \neq j. \tag{1.2}$$

Given the n integers a_i, then there is a unique solution x mod m satisfying the n congruences

$$x \equiv a_i \bmod m_i. \tag{1.3}$$

For proofs and ways of deriving the unknown x, see [2]. The second theorem that we shall use is

THEOREM 2 (Gauss). *The numbers having primitive roots are*

$$2, 4, p^n, 2p^n, \text{ where } p \text{ is an odd prime.} \tag{1.4}$$

See LeVeque [1] page 82. I wish to thank D. H. Lehmer for calling my attention to Gauss' Theorem 2.

The reader is assumed to be familiar with the beautiful theory of primitive roots and indices mod m. For the reader's convenience and also to fix our notations, we restate the main definitions.

We denote by $\varphi(m)$ the *Euler totient function* giving the number of positive integers $k \leqq m$ such that $(k, m) = 1$. The set $\{k\}$ is called a *reduced residue system* mod m (abbreviated to R.R.S. mod m).

It is known that

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right), \qquad \varphi(1) = 1. \tag{1.5}$$

A number $a > 1$ is called a *primitive root* mod m, provided that the $\varphi(m)$ powers

$$N \equiv a^I (I = 0, 1, \dots, \varphi(m) - 1) \bmod m, \tag{1.6}$$

are the elements of a R.R.S. mod m. Notice that the sequence (1.6) can not be further extended, because by Euler's theorem $a^{\varphi(m)} \equiv 1 \bmod m$.

The exponent I is called the *index* of $N \bmod m$, and we write

$$I = \operatorname{ind} N \bmod m. \tag{1.7}$$

Examples. 1. For the modulus $m = 4$ the number $a = 3$ is a primitive root, for $\varphi(4) = 2$ and the set $\{N\} = \{1, 3\}$ is a R.R.S. mod 4.

2. For $m = 25$ the number $a = 2$ is a primitive root, for $\varphi(25) = 25(1 - \frac{1}{5}) = 20$. That $N = 2^I$ $(I = 0, 1, \dots, 19)$ gives a R.R.S. mod 25 is shown by the table

(1.8)

$I = \operatorname{ind} N$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
N	1	2	4	8	16	7	14	3	6	12	24	23	21	17	9	18	11	22	19	13

From $a^{\varphi(m)} \equiv 1 \bmod m$ we see that the index I is only defined mod $\varphi(m)$. The congruences

$$I \equiv \operatorname{ind} N \bmod \varphi(m)$$

provide a one-to-one correspondence between the *multiplicative* group $\{N\}$ of a R.R.S. mod m and the *additive* group $\{I\}$ of a residue system $\{I\} \bmod \varphi(m)$. In passing to indices, a relation $N_1 \equiv N_2 N_3 \bmod m$ is changed into $\operatorname{ind} N_1 \equiv \operatorname{ind} N_2 + \operatorname{ind} N_3 \bmod \varphi(m)$; we have here a situation analogous to the logarithms of real analysis.

2. The Indices for Moduli which Admit No Primitive Roots

Our main tool is

THEOREM 3. *We make the same assumptions* (1.1), (1.2) *as in Theorem* 1, *hence, let*

$$m_i(i=1,\ldots,n), \quad all\ m_i>2, \tag{2.1}$$

be n given moduli such that

$$(m_i, m_j)=1 \quad if\ i\neq j, \qquad m=m_1m_2\cdots m_n. \tag{2.2}$$

We add the assumption that all moduli m_i admit primitive roots; more specifically, let

$$a_i \text{ be a primitive root mod } m_i \ (i=1,\ldots,n). \tag{2.3}$$

We determine the solutions b_i of the n Chinese Remainder problems

$$\begin{array}{llll} b_1\equiv a_1 \bmod m_1 & b_2\equiv 1 \bmod m_1 & \ldots & b_n\equiv 1 \bmod m_1\\ b_1\equiv 1 \bmod m_2 & b_2\equiv a_2 \bmod m_2 & \ldots & b_n\equiv 1 \bmod m_2\\ b_1\equiv 1 \bmod m_3 & b_2\equiv 1 \bmod m_3 & \ldots & b_n\equiv 1 \bmod m_3\\ \vdots & \vdots & & \vdots\\ b_1\equiv 1 \bmod m_n & b_2\equiv 1 \bmod m_n & & b_n\equiv a_n \bmod m_n. \end{array} \tag{2.4}$$

In words: The $n\times n$ matrix of the right-hand sides have all its elements $=1$, except that its diagonal has the elements $a_1, a_2,\ldots a_n$.

Then every element N of a reduced residue system mod m *is produced just once by the congruences*

$$N\equiv b_1^{x_1}b_2^{x_2}\cdots b_n^{x_n} \bmod m \quad (1\leqq N\leqq m-1), \tag{2.5}$$

where the exponents are described by

$$x_i=0,1,\ldots,\varphi(m_i)-1 \qquad (i=1,\ldots,n). \tag{2.6}$$

Proof. The number of elements of a R.R.S. mod m is $=\varphi(m)$, which equals the number of elements N produced by (2.5) and (2.6), which is $=\prod\varphi(m_i)$ in view of our assumption (2.2). We therefore obtain the correct number of elements N. We must still show that two elements

$$N\equiv b_1^{x_1}\cdots b_n^{x_n}, \qquad N'\equiv b_1^{x_1'}\cdots b_n^{x_n'} \bmod m$$

can not be congruent mod m, unless $x_i=x_i'$ $(i=1,\ldots,n)$.

We do this by contradiction: We assume that

$$(x_1,\ldots,x_n)\neq(x_1',\ldots,x_n') \tag{2.7}$$

and we are to show that (2.7) implies that

$$N\not\equiv N' \bmod m. \tag{2.8}$$

More specifically, let us assume that*

$$x_n\neq x_n' \tag{2.9}$$

and we are to prove that (2.8) holds.

Indeed, if (2.8) were wrong we would have

$$b_1^{x_1}\cdots b_n^{x_n}\equiv b_1^{x_1'}\cdots b_n^{x_n'} \bmod m,$$

*A similar proof of (2.8) holds if we replace the assumption (2.9) by $x_j\neq x_j'$ with $j<n$.

and, therefore, also

$$b_1^{x_1} \cdots b_n^{x_n} \equiv b_1^{x_1'} \cdots b_n^{x_n'} \bmod m_n. \tag{2.10}$$

However, from the last $n-1$ congruences of each of the first $n-1$ C.R. problems (2.4), we see that

$$b_j \equiv 1 \bmod m_n \quad \text{for} \quad j = 1, \ldots, n-1,$$

and so (2.10) reduces to

$$b_n^{x_n} \equiv b_n^{x_n'} \bmod m_n. \tag{2.11}$$

On the other hand, from the congruences on the "main diagonal" of the entire system (2.4) we get that

$$b_i \equiv a_i \bmod m_i$$

and so, by (2.3), we also conclude that

$$b_i \text{ is a primitive root} \bmod m_i \qquad (i = 1, \ldots, n) \tag{2.12}$$

and, in particular, that b_n is a primitive root mod m_n. This, however, shows that our assumptions (2.9) and (2.11) contradict each other. This concludes the proof of Theorem 3.

In view of Theorem 3 it seems natural to introduce the following definition. The n-dimensional vector $I = (x_1, x_2, \ldots, x_n)$, whose components appear in (2.5), is called the vector index of $N \bmod m$, or simply the index of $N \bmod m$, and we write

$$I = \operatorname{ind} N \bmod m. \tag{2.13}$$

From $b_1^{\varphi(m_i)} \equiv 1 \bmod m_i$ we see that we can add to x_i, if necessary, multiples of m_i. In this way the *multiplicative* group $\{N\}$ of order $\varphi(m_i)$ of a R.R.S. mod m is mapped one-to-one on the additive group $\{I\} = \{(x_1, \ldots, x_n)\}$ by (2.5). This mapping is explicitly described in our § 3 for the special case when $n = 2$, $m_1 = 4$, and $m_2 = 25$.

What are the moduli $m = m_1 \cdots m_n$ to which we can apply our Theorem 3? The assumptions of Theorem 3 show that we can select for the n factors m_i any of the moduli described by Gauss' Theorem 2. This establishes

COROLLARY 1. *We can apply Theorem 3 to moduli m of the form*

$$\prod_{s=1}^{l} p_s^{k_s}, \qquad 2\prod_{s=1}^{l} p_s^{k_s}, \qquad 4\prod_{s=1}^{l} p_s^{k_s}, \tag{2.14}$$

where the p_s are distinct odd primes, with $l \geq 1$.

Indeed, we can decompose each of the moduli (2.14) into relatively prime factors of the form required by Theorem 2.

3. The Modulus $m = 100$

As the simplest possible example for Theorem 3 we chose $m = 100$ with the decomposition

$$n = 2, \qquad m_1 = 4, \qquad m_2 = 25, \tag{3.1}$$

whose primitive roots are known from our examples to be

$$a_1 = 3, \qquad a_2 = 2, \text{ respectively.} \tag{3.2}$$

The C.R. problems (2.4) now become

$$\begin{aligned} b_1 &\equiv 3 \bmod 4, & b_2 &\equiv 1 \bmod 4 \\ b_1 &\equiv 1 \bmod 25, & b_2 &\equiv 2 \bmod 25, \end{aligned} \tag{3.3}$$

whose solutions are easily found to be

$$b_1 = 51, \qquad b_2 = 77. \tag{3.4}$$

The main results (2.5), (2.6) of Theorem 3 show that the congruences

$$N \equiv 51^{x_1} 77^{x_2} \bmod 100, \qquad x_1 = 0, 1, \qquad x_2 = 0, 1, \ldots, 19, \qquad (1 \leqq N \leqq 99), \tag{3.5}$$

furnish a R.R.S. mod 100.

The tables of numbers N and vector indices I are found to be

Table of numbers N

$x_1 \backslash x_2$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	1	77	29	33	41	57	89	53	81	37	49	73	21	17	9	93	61	97	69	13
1	51	27	79	83	91	7	39	3	31	87	99	23	71	67	59	43	11	47	19	63

(3.6)

Table of indices (x_1, x_2)

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

(3.7)

Table 3.6 gives the number N if ind $N = (x_1, x_2)$ is prescribed, where we locate x_1 in the first column and x_2 in the first row. Table 3.7 gives the index $I = (x_1, x_2)$ if N is given, where we locate the tens digit of N in the first column and its unit digit in the first row.

As an example, let us find the product $N = 47 \cdot 27 \bmod 100$. Passing to indices, we find $\operatorname{ind} 47 = (1, 17)$, $\operatorname{ind} 27 = (1, 1)$, and so $\operatorname{ind}(47 \cdot 27) = (1, 17) + (1, 1) = (2, 18) = (0, 18)$. The first table gives the number $69 \equiv 47 \cdot 27 \bmod 100$.

As a more interesting application let us solve the congruence

$$N^4 \equiv 61 \bmod 100. \tag{3.8}$$

We pass to indices on both sides of the congruence setting ind $N=(x_1, x_2)$. From the second table we find ind 61 = (0, 16). We obtain

$$4(x_1, x_2) \equiv (0,16) \; (\operatorname{mod} 2, \operatorname{mod} 20),$$

which gives the two congruences

$$4x_1 \equiv 0 \operatorname{mod} 2, \qquad 4x_2 \equiv 16 \operatorname{mod} 20.$$

The first congruence has the two solutions $x_1 = 0, 1$, and the second the four solutions $x_2 = 4$, 9, 14, 19. This gives the eight different indices

$$(x_1, x_2) = (0,4), (0,9), (0,14), (0,19), (1,4), (1,9), (1,14), (1,19).$$

TABLE 3.6 gives the corresponding numbers and shows that (3.8) has the eight solutions $N = 41$, 37, 9, 13, 91, 87, 59, 63, hence,

$$N = 9, 13, 37, 41, 59, 63, 87, 91, \tag{3.9}$$

which is readily checked on a hand-held calculator.

4. A Circular Slide Rule for the Modulus 100

If the modulus m has a primitive root, then the mapping $\{N\} \leftrightarrow \operatorname{ind} N$ is an isomorphism between the multiplicative group mod m, and the additive group mod $\varphi(m)$. The operations on the latter are nicely performed mechanically on a circular slide rule. I can find no reference to this mechanical device, the only notable exception being B. M. Stewart's book [3], where the slide rule mod 29 is described in chapter 20. Notice the prime modulus $m = 29$ admits the primitive root $a = 2$.

For a modulus $m \doteq m_1 m_2$, to which we can apply Theorem 3 with $n = 2$, the operations of the additive group of

$$\operatorname{ind} N = (x_1, x_2) \; (\operatorname{mod} \varphi(m_1), \operatorname{mod} \varphi(m_2))$$

can no longer be performed on a circular slide rule. A notable exception is our modulus $m = 100 = 4 \cdot 25$ for the following reason: Here $\varphi(4) = 2$, and the operations on x_1 mod 2 can be done mentally, without mechanical aid.

The slide rule mod 100 is shown in FIGURE 1. It shows five increasing concentric circles $C_1, \ldots, C_5$, each divided in 20 equal arcs. The slide rule must explicitly contain the 1–1 correspondence between the set $\{N\}$ of $\varphi(100) = 40$ numbers and the set $\{I\} = \{(x_1, x_2)\}$ of 40 indices.

Along the points on C_1 and C_5 we place the 20 values of $x_2 = 0, 1, \ldots, 19$. Along every radius, like $x_2 = 3$, say, we place the corresponding values of x_1 and N, which are $x_1 = 0$, $N = 33$, and $x_1 = 1$, $N = 83$, respectively, which we find from TABLE 3.6. The values 0, 33 are placed along C_4 and C_3, respectively, and we repeat them symmetrically with respect to C_3; likewise we place 1 and 83 near the radius of $x_2 = 3$, and repeat them by symmetry in C_3.

5. Construction of the Slide Rule

We glue FIGURE 1 on a piece of cardboard and cut the figure along the circle C_3 obtaining a disk D and a ring R. We glue the ring R onto a piece of cardboard and

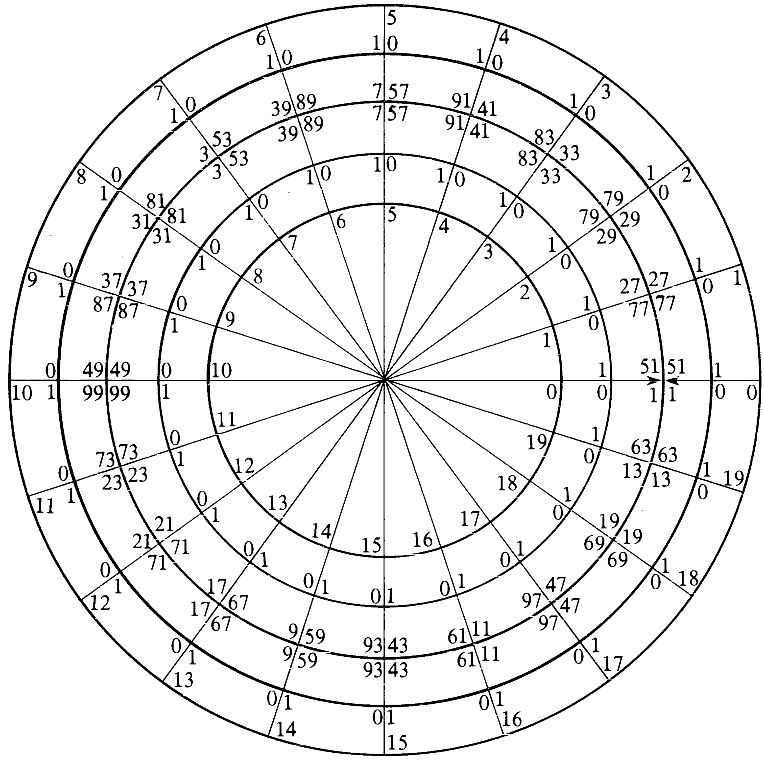


FIGURE 1
A circular slide rule mod 100.

restore the disk D to its old place, with a pin in its center so that the disk can turn about its center. We also mark its initial position, for $x_2 = 0$, by two arrowheads. The slide rule so obtained performs multiplications and division mod 100 mechanically.

An example. To find $79 \times 37 \bmod 100$, we locate 79 on C_3 and turn the disk by two divisions counterclockwise until the initial arrowhead points to 79. The number 37 on the disk now points to the pair of possible products 73 and 23. Since for $N = 79$ we have $x_1 = 1$ and for 37 we have $x_1 = 0$, we conclude that for their product we have $x_1 = 1 + 0 = 1 \bmod 2$. This is why we select $N = 23$ rather then 73, and so

$$79 \times 37 = 23 \bmod 100. \tag{5.3}$$

How did it work? The answer: From the slide rule we see that for $N = 79$ we have $x_2 = 2$, and for $N = 37$ we have $x_2 = 9$; therefore, for their product we have $x_2 = 2 + 9 = 11 \bmod 20$: On the slide rule we performed the addition $2 + 9 = 11$. Thus for the product $x_2 = 11$; and this gave the possible products 73 or 23.

REFERENCES

1. W. J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley Publishing Co., 1977.
2. I. J. Schoenberg, The Chinese Remainder Theorem and polynomial interpolation, *College Math. J.* 18 (1987), 320–22.
3. B. M. Stewart, *Theory of Numbers*, second edition, Macmillan, New York, 1964.

Point and Circle Configurations; A New Theorem

HAROLD L. DORWART
Trinity College
Hartford, Connecticut 06106

Several of the n_3 self-dual point and line configurations—n points, n lines, 3 points on a line, 3 lines through a point—are well known, e.g., the 9_3 figure that illustrates the theorem of Pappus, and the 10_3 figure that illustrates the theorem of Desargues. (The "self-dual" comes from the fact that "point" and "line" can be interchanged in the above description without changing the meaning.) More general point and line configurations, ones that are not self-dual, occur as illustrations of many other projective geometry theorems. Some of these, such as the following, appear to be very complicated, but they give an idea of the type of investigation that interested geometers in the late nineteenth century.

> Nine points, located in sets of three each on three concurrent lines, form 36 sets of three perspective triangles. For each set of three distinct triangles the axes of perspectivity meet in a point; and the 36 points thus obtained lie in sets of four on 27 lines, thus giving a $36_3 27_4$ configuration (i.e. 36 points, 27 lines, 3 lines through each point, 4 points on each line.)

That point and line configurations appear elsewhere than as illustrations of geometric theorems is evident from FIGURE 1, which is taken from an advertisement for a current book on turbulence [3]. If one ignores the arrows, this figure is that of a $6_5 15_2$ point and line configuration.

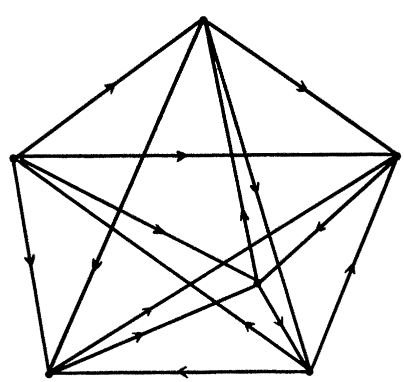


FIGURE 1

It appears that point and circle configurations are not well known (if they are known at all), and—after these introductory paragraphs—the remainder of this paper will be devoted to a brief discussion of Clifford's chain of theorems [1], and Miquel's theorem [4], whose diagrams exhibit such configurations. The paper will conclude with what is believed to be a new theorem—one similar to that of Miquel.

CLIFFORD'S FIRST THEOREM. *Let C_1, C_2, C_3, C_4 be four circles of general position through a point P_0. Let P_{ij} be the second intersection of the circles C_i and C_j. Let P_{ijk} denote the circle $P_{ij}P_{ik}P_{jk}$. Then the four circles C_{234}, C_{134}, C_{124}, C_{123} all pass through one point P_{1234}.*

CLIFFORD'S SECOND THEOREM. *Let C_5 be a fifth circle through P_0. Then the five points P_{2345}, P_{1345}, P_{1245}, P_{1235}, P_{1234} all lie on one circle C_{12345}.*

CLIFFORD'S THIRD THEOREM. *The six circles C_{23456}, C_{13456}, C_{12456}, C_{12356}, C_{12346}, C_{12345} all pass through one point P_{123456}.*

And thus the chain continues, with the closure taking place alternately on a point or on a circle.

FIGURE 2 illustrates Clifford's First Theorem and, since it consists of 8 points and 8 circles with 4 circles on each point and 4 points on each circle, it can be called a self-dual point and circle configuration 8_4. Likewise FIGURE 3 (constructed 60 years ago by the writer when he was a graduate student*) is a similar 16_5 configuration. Thus theorems of the Clifford chain are represented by $(2^{n-1})_n$ point and circle configurations, where n is the number of circles drawn through the starting point P_0.

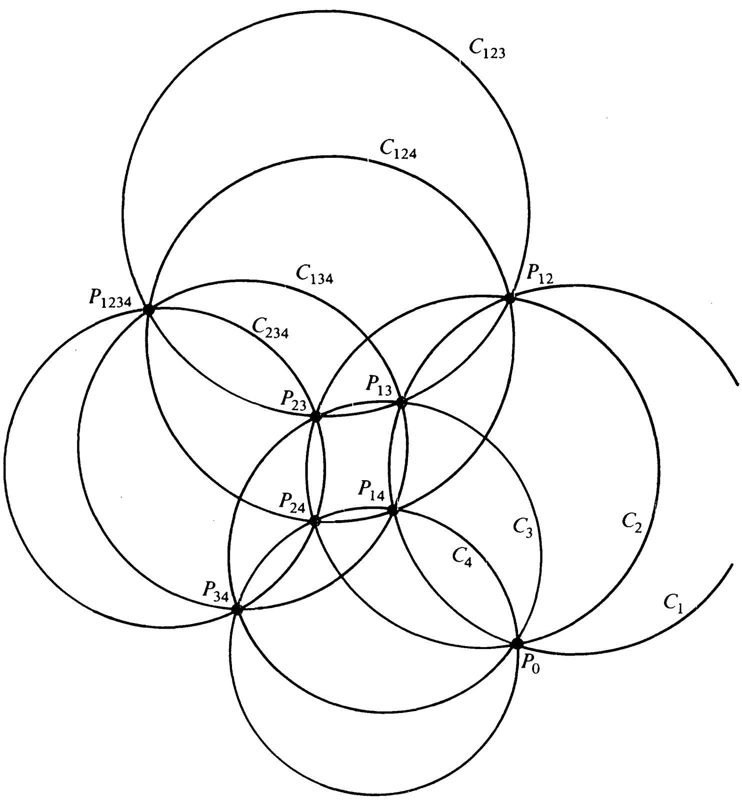


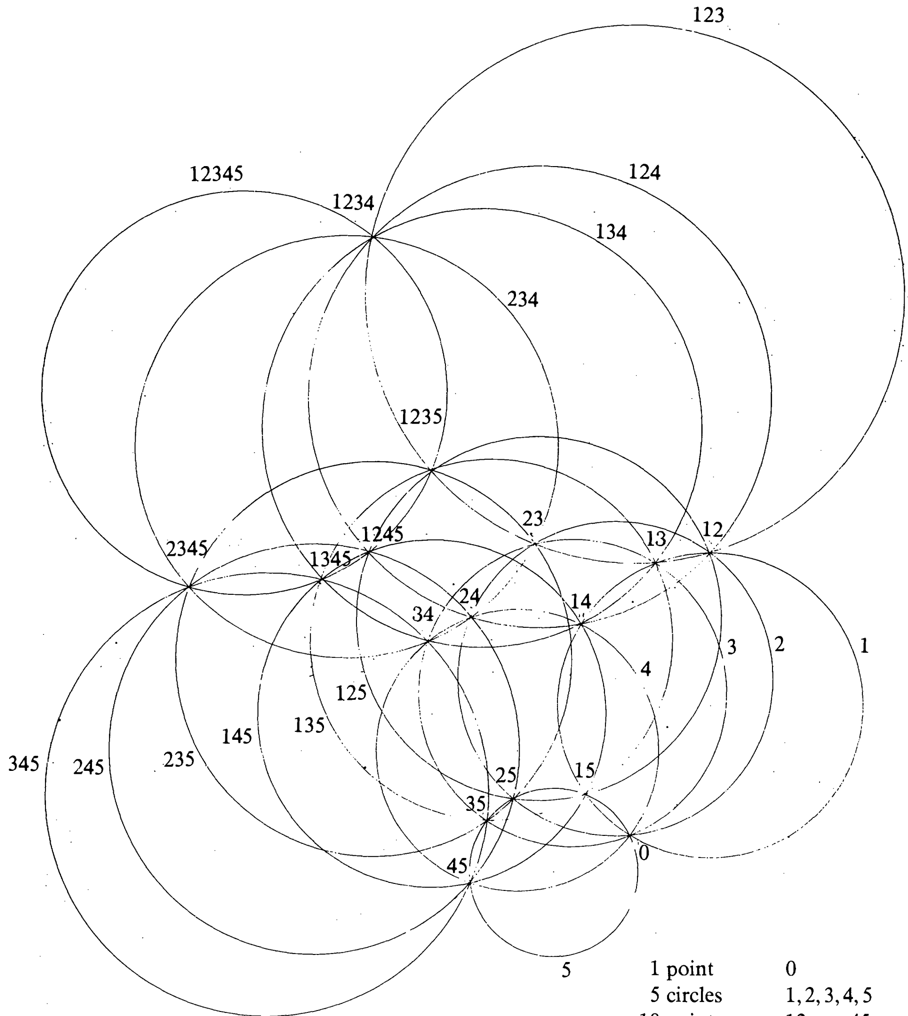
FIGURE 2

The reader may be interested in considering why Clifford's first theorem begins with four circles through P_0 instead of three. FIGURE 4 illustrates the case of three circles and shows that it describes a trivial situation. Since three noncollinear points always lie on a circle, the Clifford conclusion (that P_{12}, P_{13}, P_{23} lie on a circle) is

*To the accompaniment of "A drawing a day keeps the doctor's degree away" from a fellow student who had no interest in geometry.

Clifford Configuration for 5 Circles

16 points, 16 circles
Each point on 5 circles
Each circle on 5 points



1 point	0
5 circles	1, 2, 3, 4, 5
10 points	12, ..., 45
10 circles	123, ..., 345
5 points	2345, ..., 1234
1 circle	12345

FIGURE 3

obvious. Several interesting observations, however, can be made from FIGURE 4. Consider the following table.

P_0	P_0	P_0	P_{12}
P_{12}	P_{12}	P_{13}	P_{13}
P_{13}	P_{23}	P_{23}	P_{23}

This table represents a type of block design known as a *biplane*. If we consider the elements of this design to represent points, and the columns to represent the three

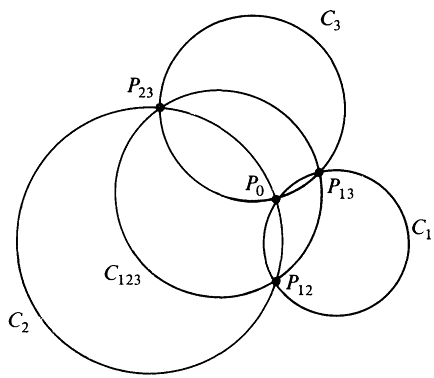


FIGURE 4

points on each of the four circles C_1, C_2, C_3, C_{123}, then FIGURE 4—which is the geometric representation for the 4_3 point and circle configuration of our trivial theorem—is also a geometric representation for this biplane. And, since three noncollinear points always determine a plane (as well as a circle), another geometric representation for the biplane is in terms of a point and plane configuration in space. FIGURE 5—a tetrahedron with edges (dotted lines) ignored—shows this representation. It is a self-dual point and plane configuration, 4 points (vertices), 4 planes (faces), 3 planes on each point, and 3 points on each plane.**

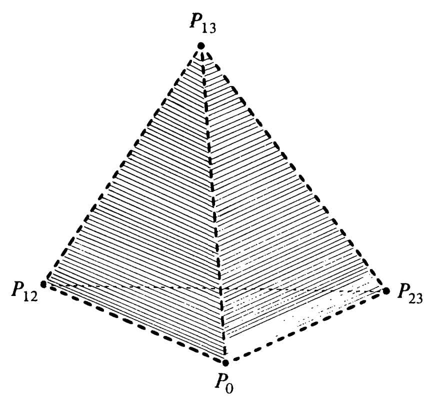


FIGURE 5

Self-dual point and circle configurations having been displayed, a theorem of Miquel will now be used to show the existence of a point and circle configuration that is not self-dual. For a reason that will be apparent later, this theorem will be written in detailed form.

MIQUEL'S THEOREM. *Take four points labeled* 1, 8, 3, 6 *on a circle* C_1 (*see* FIGURE 6). *Then label another circle on* (*i.e. through*) *points* 1 *and* 8 *as* C_5, *an additional circle on points* 8 *and* 3 *as* C_2, *an additional circle on points* 3 *and* 6 *as* C_3, *and a*

**It may be of interest, historically, to note that Th. Reye mentions 8_4 and 16_5 point and plane configurations in a paper published in 1882—the same year in which W. K. Clifford published a special form of his point and circle theorems. Earlier, in his *Geometrie der Lage* (1876), Reye was the first to use the term *configuration* as it is currently used in geometry.

final circle on points 6 *and* 1 *as* C_4. *Now label a second point common to circles* C_3 *and* C_2 *as* 5, *a second point common to circles* C_2 *and* C_5 *as* 2, *a second point common to circles* C_5 *and* C_4 *as* 7, *and a second point common to circles* C_4 *and* C_3 *as* 4. *Then the points* 5, 2, 7, 4 *will all lie on a circle* C_6.

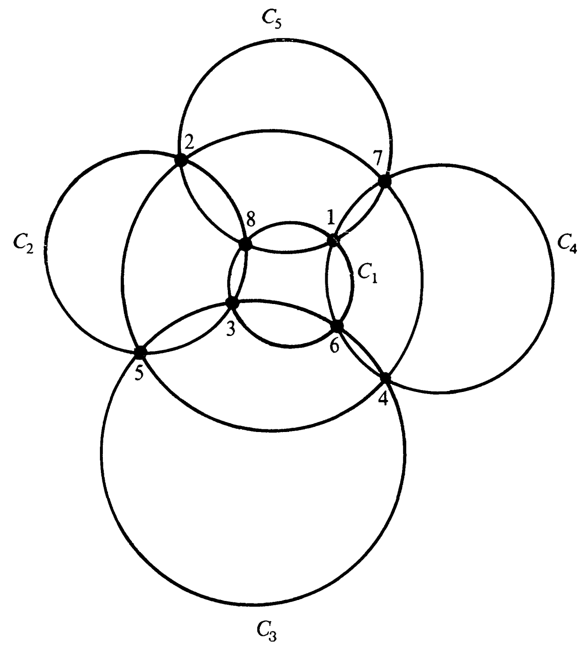


FIGURE 6

FIGURE 6 is that of an $8_3 6_4$ point and circle configuration, i.e., 8 points, 6 circles, 3 circles on each point, and 4 points on each circle. There are other ways of stating the above theorem (which is an important one in Inversive Geometry [2]), but the way used (adapted from [4]) gives the following neat description of FIGURE 6. In the four-by-two array of the eight points

1	2	3	4
5	6	7	8

any two points of a row and the non-corresponding points of the other row are on a circle.

If the reader recalls the earlier observation that three noncollinear points determine not only a circle but also a plane, he or she can quickly see that the 8 points and 6 circles of Miquel translate into an 8 point, 6 plane representation, i.e., the FIGURE 7 drawing of a cube where the edges are ignored. But such a space figure has a point and plane dual figure, i.e., a $6_4 8_3$ configuration—the octahedron which is shown in FIGURE 8. This implies that Miquel's theorem has a point and circle dual theorem (apparently not previously recognized) which is quickly stated by interchanging the words point and circle in Miquel's theorem as follows.

THE NEW THEOREM. *Take four circles* C_1, C_8, C_3, C_6 *on a point* 1 (*see* FIGURE 9). *Then label another point on circles* C_1 *and* C_8 *as* 5, *an additional point on circles* C_8 *and* C_3 *as* 2, *an additional point on circles* C_3 *and* C_6 *as* 3, *and a final point on circles* C_6 *and* C_1 *as* 4. *Now label a second circle common to points* 3 *and* 2 *as* C_5, *a second*

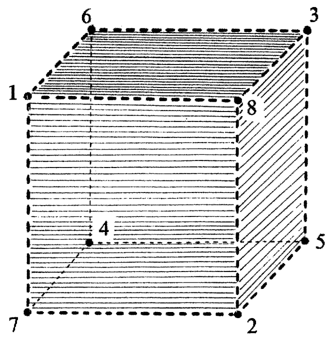


FIGURE 7

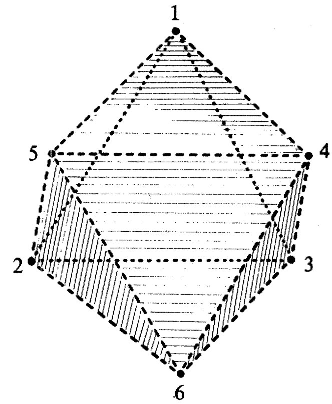


FIGURE 8

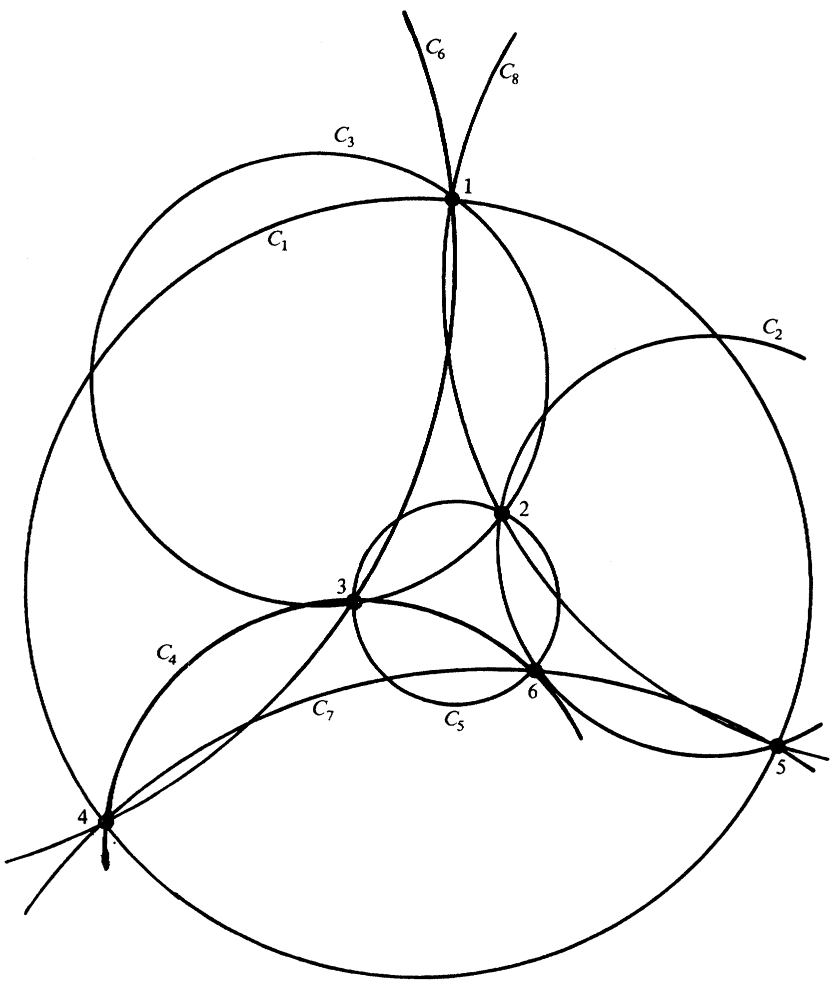


FIGURE 9

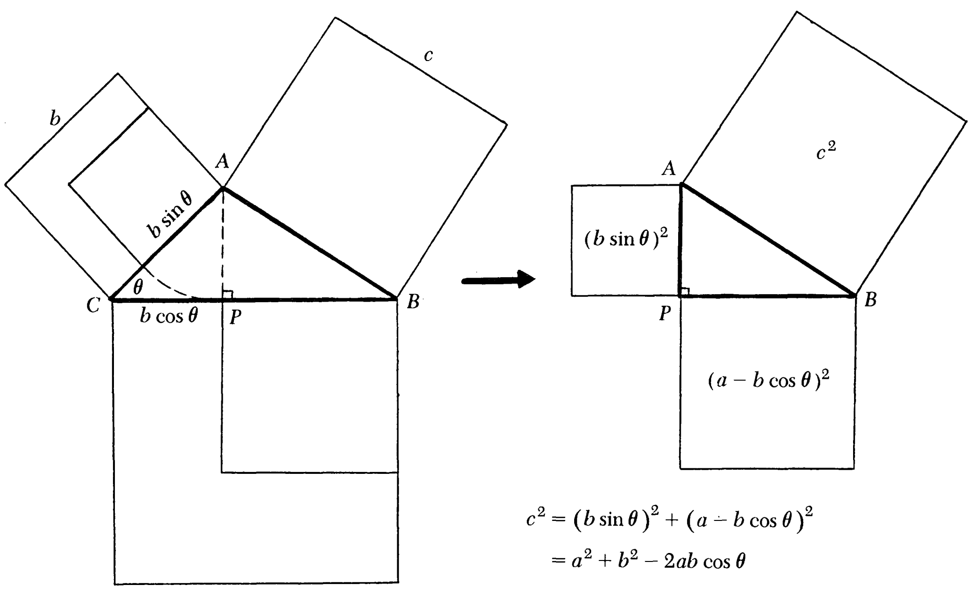
circle common to points 2 *and* 5 *as* C_2, *a second circle common to points* 5 *and* 4 *as* C_7, *and a second circle common to points* 4 *and* 3 *as* C_4. *Then the circles* C_5, C_2, C_7, C_4 *all pass through a point* 6.

The two remaining Platonic solids are point and plane duals of each other, the icosahedron a $12_5 20_3$ point and plane configuration and the dodecahedron a $20_3 12_5$ configuration. Do point and circle theorems that correspond to these exist? This question is left for the reader to investigate.

REFERENCES

1. H. S. M. Coxeter, *Introduction to Geometry*, John Wiley & Sons, 1961, p. 262.
2. P. Dembowski, *Finite Geometries*, Springer-Verlag, 1968, pp. 255–280.
3. D. L. Dwoyer, M. Y. Hussaini, R. G. Voigt, editors, *Theoretical Approaches to Turbulence* (Applied Mathematical Sciences, Volume 58), Springer-Verlag, 1985.
4. F. Morley and F. V. Morley, *Inversive Geometry*, Ginn & Company, 1933.

Proof without Words: Law of Cosines for $\theta < \pi/2$



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

—TIMOTHY A. SIPKA
Anderson University
Anderson, IN 46012

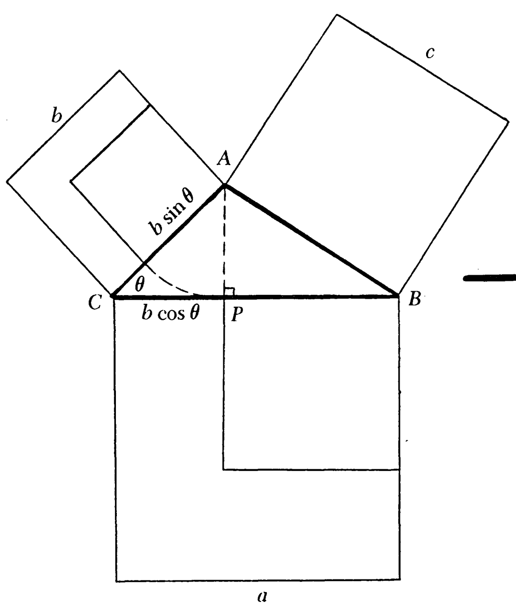
circle common to points 2 *and* 5 *as* C_2, *a second circle common to points* 5 *and* 4 *as* C_7, *and a second circle common to points* 4 *and* 3 *as* C_4. *Then the circles* C_5, C_2, C_7, C_4 *all pass through a point* 6.

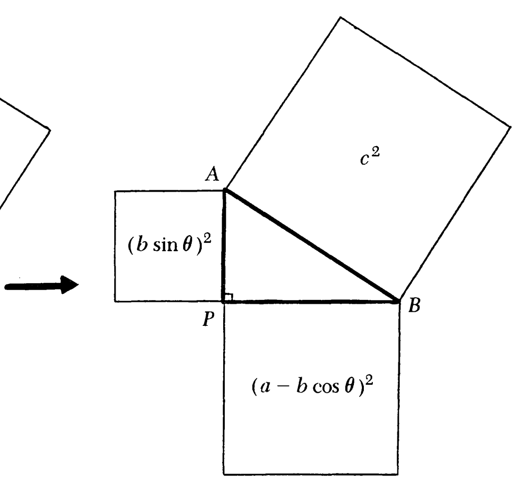
The two remaining Platonic solids are point and plane duals of each other, the icosahedron a $12_5 20_3$ point and plane configuration and the dodecahedron a $20_3 12_5$ configuration. Do point and circle theorems that correspond to these exist? This question is left for the reader to investigate.

REFERENCES

1. H. S. M. Coxeter, *Introduction to Geometry*, John Wiley & Sons, 1961, p. 262.
2. P. Dembowski, *Finite Geometries*, Springer-Verlag, 1968, pp. 255–280.
3. D. L. Dwoyer, M. Y. Hussaini, R. G. Voigt, editors, *Theoretical Approaches to Turbulence* (Applied Mathematical Sciences, Volume 58), Springer-Verlag, 1985.
4. F. Morley and F. V. Morley, *Inversive Geometry*, Ginn & Company, 1933.

Proof without Words: Law of Cosines for $\theta < \pi/2$





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

—Timothy A. Sipka
Anderson University
Anderson, IN 46012

PROBLEMS

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

BRUCE HANSON, *associate editor*
St. Olaf College

Proposals

To be considered for publication, solutions should be received by April 1, 1989.

1302. *Proposed by W. E. Briggs, University of Colorado, Boulder, Colorado.*

Show, for integral $n \geqslant 3$, that

$$\zeta(n) \equiv \sum_{r=1}^{\infty} \frac{1}{r^n} = \sum_{i=1}^{n-2} \sum_{p,q=1}^{\infty} \frac{1}{p^i(p+q)^{n-i}}.$$

1303. *Proposed by George T. Gilbert, St. Olaf College, Northfield, Minnesota.*

Find all continuous functions f on $(0, \infty)$ such that

$$\int_x^{x^2} f(t)\,dt = \int_1^x f(t)\,dt \quad \text{for all } x > 0.$$

1304. *Proposed by William Moser, McGill University, Montreal, Canada.*

For nonnegative integers, k, n, establish the identity

$$\sum_{i \geqslant 0} (-1)^i \binom{n-k+1}{i} \binom{n-3i}{n-k} = \sum_{i \geqslant 0} \binom{n-k+1}{i} \binom{i}{k-i}.$$

(Here, $\binom{n}{k} = 0$ when $k < 0$ or $k > n$.)

ASSISTANT EDITORS: Clifton Corzatt, George Gilbert, and Theodore Vessey, *St. Olaf 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 C. Larson, Department of Mathematics, St. Olaf College, Northfield, MN 55057.

1305. *Proposed by H. Demir and C. Tezer, Middle East Technical University, Ankara, Turkey.*

Let $P_0 = B, P_1, P_2, \ldots, P_n = C$ be points, taken in that order, on the side BC of the triangle ABC. If r, r_i and h denote respectively the inradii of the triangles ABC, $AP_{i-1}P_i$ and the common altitude, prove that

$$\prod_{i=1}^{n}\left(1-\frac{2r_i}{h}\right)=1-\frac{2r}{h}.$$

1306. *Proposed by Carl G. Wagner, The University of Tennessee, Knoxville, Tennessee.*

Given the formal power series

$$C(x)=\sum_{n=1}^{\infty} c(n)x^n,$$

with $c(n) \geqslant 0$ for all $n \geqslant 1$, define the sequence $(d(n))_{n=0}^{\infty}$ by

$$(1-C(x))^{-1}=\sum_{n=0}^{\infty} d(n)x^n \equiv D(x).$$

Prove that $d(n) > 0$ for all n sufficiently large if and only if the ideal generated by $S = \{n\colon c(n) > 0\}$ is equal to the set of integers.

Quickies

Answers to the Quickies are on page 265.

Q736. *Proposed by William P. Wardlaw, U.S. Naval Academy, Annapolis, Maryland.*

Let p be a fixed prime and n a fixed positive integer. What is the probability that an $n \times n$ matrix $\mathbf{A}$ with randomly chosen integer entries has determinant divisible by p?

Q737. *Proposed by Murray S. Klamkin, University of Alberta, Edmonton, Canada.*

Determine $P_n(n^2)$ where

$$P_n(x)=\frac{(x-1^2)}{2!^2}-\frac{(x-1^2)(x-2^2)}{3!^2}+\cdots+\frac{(-1)^n(x-1^2)(x-2^2)\cdots\left(x-(n-1)^2\right)}{n!^2}.$$

Q738. *Proposed by Sidney Kung, Jacksonville University, Florida.*

Let $f(x)$ be continuous on the closed interval $[-1,1]$ and differentiable in the open interval $(-1,1)$. If $f(1)=0$ and if $f(x)>0$ for $x \in (-1,1)$, show that for any positive real numbers r and s, there is a number $c \in (-1,1)$ such that $rf(c)f'(-c) = sf'(c)f(-c)$.

Solutions

Prime Gaps **October 1987**

1272. *Proposed by Jerrold W. Grossman, Oakland University, Michigan, and Allen J. Schwenk, Western Michigan University.*

For n a positive integer, let $f(n)$ be the smallest prime number p such that $n+p$ is also prime, if such a p exists, and 0 otherwise. Show that f is unbounded.

I. *Solution by The Oxford Running Club, The University of Mississippi.*

Let p be a prime. Since there are arbitrarily large gaps in the sequence of primes, we may let q be any prime which immediately follows a sequence of at least p composites. Then $f(q-p)=p$. This shows that f maps onto the sequence of prime numbers. (Also, note that $f(7)=0$, because for every prime p, $7+p$ is composite.)

II. *Solution by the Con Amore Problem Group, Royal Danish School of Educational Studies, Copenhagen, Denmark.*

More generally: Let P be an arbitrary set of positive integers, and let Q be an infinite set of positive integers with arbitrarily large "gaps"; i.e., there are in the set of positive integers arbitrarily long sequences of consecutive numbers not belonging to Q. For n a positive integer, let $f(n)$ be the smallest number p in P such that $n+p$ is in Q, if such a p exists, and 0 otherwise. Then the set of values of f is P, or P with 0 thrown in.

Proof. Let p be a number in P, and let

$$m, m+1, m+2, \ldots, m+p-1$$

be p consecutive positive integers not in Q; let q be the first number in Q among the numbers

$$m+p, m+p+1, m+p+2, \ldots,$$

and let $n=q-p$. Then none of

$$n+1, n+2, n+3, \ldots, q-1$$

is in Q, but q is, and consequently, $f(n)=p$.

Also solved by Mangho Ahuja, C. K. Bailey and R. B. Richter, S. F. Barger, Mark Bowron, Duane M. Broline, Nicholas Buck (Canada), Onn Chan (student), Rick Chase, Thomas Dick, Robert L. Doucette, Thomas E. Elsner, Richard B. Evans, Enzo R. Gentile (Argentina), Cornelius Groenewoud, Michael B. Handelsman, G. A. Heuer (Austria), S. Holmes, C. B. Khare and J. Levy (England), David W. Koster, John W. Krussel, Eugene Levine, Bill Mixon, Leonard L. Palmer, Robert Sheets, Shippensburg University Mathematical Problem Solving Group, Raul A. Simon (Chile), Man-Keung Siu and Kai-Man Tsang (Hong Kong), Florentin Smarandache (Romania), Blair Spearman (Canada), J. M. Stark, Garrett R. Vargas (student), Charles H. Webster, Eric Wepsic (student), and the proposers. There were three incomplete solutions and three incorrect solutions.

Conditions for Integer Recurrence **October 1987**

1273. *Proposed by Benjamin G. Klein, Davidson College, North Carolina, and John Layman, Virginia Polytechnic Institute and State University.*

Let q be a positive integer and let p be a prime. Let $f_0=f_1=f_2=p$ and define f_n for $n>2$ by

$$f_{n+1}=(f_n f_{n-1}+q)/f_{n-2}.$$

a. Prove that if p is odd, then f_n is an integer for all n if and only if p^2 divides q.
b. Prove that if $p=2$, then f_n is an integer for all n if and only if p divides q.

Solution by J. C. Binz, University of Bern, Switzerland.

Since $f_{n+1}f_{n-2}-f_n f_{n-1}=q$ for all $n\geqslant 2$, we have

$$f_{n+2}=\frac{f_{n+1}f_n+q}{f_{n-1}}=\frac{f_{n+1}f_n+f_{n+1}f_{n-2}-f_n f_{n-1}}{f_{n-1}}=\frac{f_{n+1}(f_n+f_{n-2})}{f_{n-1}}-f_n,$$

and, therefore,

$$\frac{f_{n+2}+f_n}{f_{n+1}}=\frac{f_n+f_{n-2}}{f_{n-1}}=\cdots=\begin{cases}(f_2+f_0)/f_1=2 & (n\text{ even}),\\ (f_3+f_1)/f_2=2+q/p^2 & (n\text{ odd}).\end{cases}$$

Suppose p is an odd prime. If $q=kp^2$, k an integer, then $f_{n+2}=cf_{n+1}-f_n$ with alternatively $c=2$ or $c=2+k$. Since f_0 and f_1 are integers, all f_n are integers. For the "only if," we find that

$$f_5=p+\frac{2q}{p}\left(2+\frac{q}{p^2}\right).$$

This shows that if f_5 is an integer, p^2 divides q.

Suppose that $p=2$. If $q=2k$, k an integer, then $f_{n+2}=2f_{n+1}-f_n$ for n even shows that f_{2m} are even integers. Further, $f_{n+2}=(2+k/2)f_{n+1}-f_n$ for n odd proves that all f_{2m+1} are integers. In the other direction, note that if f_3 $(=2+q/2)$ is an integer, then 2 divides q.

Also solved by Tamer Adanir (Turkey), C. K. Bailey and R. B. Richter, Duane M. Broline, Con Amore Problem Group (Denmark), Lorraine L. Foster, J. Heuver (Canada), Michael Vowe (Switzerland), Eric Wepsic (student), and the proposers.

Application of Rolle's Theorem **October 1987**

1274. *Proposed by S. Kung, Jacksonville University, Florida.*

Let $f(x)$ be continuous on the closed interval $[a,b]$ and differentiable in the open interval (a,b). If $f(a)=f(b)=0$ and $f(x)>0$ for $x\in(a,b)$, show that for any positive real number r there is a number $c\in(a,b)$ such that $rf'(c)+f(c)=0$.

Two solutions by R. P. Boas, Northwestern University, Evanston, Illinois.

I. We can obtain the same conclusion for all $r\neq 0$, and the hypothesis $f(x)>0$ can be replaced by $f(x)\not\equiv 0$.

Define $g(x)=e^{x/r}f(x)$. Then g satisfies the same hypotheses as f. By Rolle's theorem, $g'(c)=0$ for some c, $a<c<b$. But $rg'(c)=e^{c/r}(rf'(c)+f(c))$, and $e^{c/r}\neq 0$, so $rf'(c)+f(c)=0$.

II. With the original hypotheses, consider $h(x)=\log f(x)$. Then $h(x)\to-\infty$ as $x\to a$ or b, and it follows that $h'(x)$ takes arbitrarily large and arbitrarily small values. Since derivatives have the intermediate value property, $h'(x)=f'(x)/f(x)$ takes all real values, and in particular the value $-1/r$, $(r\neq 0)$. Since $f'(c)/f(c)=-1/r$, $rf'(c)+f(c)=0$.

Also solved by Mangho Ahuja, C. K. Bailey and R. B. Richter, Seung-Jin Bang (Korea), S. F. Barger, *Francisco Bellot (Spain), J. C. Binz (Switzerland), Mark Bowron, Paul Bracken (Canada), Duane M. Broline, Nicholas Buck (Canada), Bruce R. Caine, Chico Problem Group, J. D. Child, Phil Clarke, Con Amore Problem Group (Denmark), Bruce Dearden, Charles Diminnie and Harry Sedinger, David Doster, Robert L. Doucette, W. O. Egerland and Charles Hansen, Alberto Facchini (Italy), Gordon Fisher, Joe Flowers, T. E. Gantner, Samuel Gehre-Egziabher (student), Enzo R. Gentile (Argentina), Ray Haertel, Lee O. Hagglund, Michael B. Handelsman, Francis M. Henderson, J. Heuver (Canada), P. L. Hon (Hong Kong), J. Howard, Stavru Hristos (Greece), Richard A. Jacobson, Richard Johnsonbaugh, Geoffrey A. Kandall, Ralph E. King, Emil F. Knapp, Robert L. Lamphere, Deborah Lawrence and David Bonner (students), Kee-Wai Lau (Hong Kong), Eugene Levine, David E. Manes, Beatriz Margolis (France), Helen M. Marston, Patrick Dale McCray, Howard Morris, Roger B. Nelsen, Stephen Noltie, The Northern Kentucky University Problem Solving Group Gene M. Ortner, Michael Pape (student), Richard E. Pfiefer, M. Riazi-Kermani, Rolf Rosenkranz, Harry D. Ruderman, H.-J. Seiffert (West Germany), M. Selby (Canada), Zun Shan and Edward T. H. Wang, Shippensburg University Mathematical Problem Solving Group, Raul A. Simon (Chile), J. M. Stark, Gerald Thompson, Nora S. Thornber, Mohan Tikoo, Michael Vowe (Switzerland), Robert J. Wagner, Eric Wepsic (student), and the proposer.*

Several people pointed out that this problem appears in the literature in a more general form, for example, in Apostol's *Mathematical Analysis*, 2nd ed., Addison-Wesley, Exercise 5.18, p. 123.

Recursive Sequence and Series **October 1987**

1275. *Proposed by Fouad Nakhli, American University of Beirut.*

Let c be a positive real number, let $a_1 = c$ and for $n \geqslant 1$, $a_{n+1} = c^{1/a_n}$.

a. Show that the sequence (a_n) converges if $0 < c \leqslant 1$.

b. Show that the series $\sum_{n=1}^{\infty} a_n$ converges if $0 < c < (1/e)^{1/e}$.

Solution by Kee-Wai Lau, Hong Kong.

a. It is clear that $a_n > 0$ for $n \geqslant 1$. Because $0 < c \leqslant 1$ we have $a_1 = c \geqslant c^{1/c} = c^{1/a_1} = a_2$. Assume, inductively, that $a_{k-1} \geqslant a_k$. Then $a_k = c^{1/a_{k-1}} \geqslant c^{1/a_k} = a_{k+1}$. It follows that the sequence (a_n) is a nonincreasing sequence bounded below by 0, and therefore converges.

b. From part a, (a_n) converges for $0 < c < (1/e)^{1/e}$. Let $L \equiv \lim_{n \to \infty} a_n$, and suppose that $L > 0$. The defining equation implies that $L = c^{1/L}$. It is straightforward to show that $x^x \geqslant (1/e)^{1/e}$ for $x > 0$. Thus, $c = L^L \geqslant (1/e)^{1/e}$, a contradiction. This shows that $L = 0$. It follows that

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = \lim_{n\to\infty} \frac{c^{1/a_n}}{a_n} = \lim_{x\to 0^+} \frac{c^{1/x}}{x} = \lim_{y\to\infty} y e^y = 0,$$

and therefore the series $\sum_{n=1}^{\infty} a_n$ converges by the ratio test.

Also solved by C. K. Bailey and R. B. Richter, Paul Bracken, Duane M. Broline, David Callan, Chico Problem Group, Phil Clarke, Con Amore Problem Group (Denmark), ITT Kanpur Problem Solving Group (India), Václav Konečný, L. Kuipers (Switzerland), Robert L. Lamphere, Beatriz Margolis (France), G. M. Ortner, Stephen Noltie, J. M. Stark, Michael Vowe (Switzerland), and the proposer. There was one incorrect solution.

Symmetric Matrix of Binomial Coefficients **October 1987**

1276. *Proposed by Lawrence J. Wallen, University of Hawaii.*

Let **A** be the $(n+1) \times (n+1)$ symmetric matrix whose (i, j)th entry is $\binom{i+j}{i}$, $i, j = 0, 1, 2, \ldots, n$. Let the characteristic polynomial $p(\lambda)$ of **A** be

$$a_0\lambda^{n+1} + a_1\lambda^n + a_2\lambda^{n-1} + \cdots + a_{n+1} \qquad (a_0 = 1).$$

Show that

$$a_j = (-1)^{n+1} a_{n+1-j}, \qquad j = 0, 1, \ldots, n+1.$$

Solution by C. K. Bailey, Mitch Baker, and R. B. Richter, U.S. Naval Academy, Annapolis.

We prove that $\det(x\mathbf{I}-\mathbf{A})=\det(x\mathbf{A}-\mathbf{I})$. This is sufficient to solve the stated problem, since $\det(x\mathbf{A}-\mathbf{I})=x^{n+1}\det(\mathbf{A}-(1/x)\mathbf{I})=(-1)^{n+1}x^{n+1}\det((1/x)\mathbf{I}-\mathbf{A})$. Thus, if $p(x)=\det(x\mathbf{I}-\mathbf{A})$, then $p(x)=(-1)^{n+1}x^{n+1}p(1/x)$, which is equivalent to the stated problem.

Let $\mathbf{A}=(\alpha_{ij})$ be a square matrix. Define the matrix $\mathbf{A}'$ to be $((-1)^{i+j}\alpha_{ij})$. From the definitions of matrix multiplication and determinant, it is trivial to verify that $(\mathbf{AB})'=\mathbf{A}'\mathbf{B}'$ and $\det(\mathbf{A}')=\det(\mathbf{A})$.

Let $\mathbf{P}$ be the $(n+1)\times(n+1)$ matrix whose (i,j)th entry is the binomial coefficient $\binom{i}{j}$, where $\binom{i}{j}$ is defined to be 0 if $i<j$. Then $\mathbf{A}=\mathbf{PP}^t$ and $\mathbf{PP}'=\mathbf{I}$, so $\mathbf{P}^{-1}=\mathbf{P}'$. (See J. Riordan, *Combinatorial Identities*, John Wiley & Sons, New York, 1968, Equation 3a, p. 8 and Example 2, p. 4.)

Since $\mathbf{P}$ is lower triangular with 1's down the diagonal, $\det(\mathbf{P})=1$; thus, $\det(\mathbf{A})=1$. Now $\det(x\mathbf{I}-\mathbf{A})=\det(x\mathbf{I}-\mathbf{PP}^t)=\det(\mathbf{P}(x\mathbf{P}'\mathbf{P}'^t-\mathbf{I})\mathbf{P}^t)=\det(x\mathbf{P}'\mathbf{P}'^t-\mathbf{I})\det(\mathbf{PP}^t)=\det(x(\mathbf{PP}^t)'-\mathbf{I})=\det(x\mathbf{A}'-\mathbf{I})=\det((x\mathbf{A}-\mathbf{I})')=\det(x\mathbf{A}-\mathbf{I})$.

Also solved by J. Binz (Switzerland), David Callan, Lorraine L. Foster, and the proposer.

Answers

Solutions to the Quickies on p. 261.

A736. The probability that p divides $\det(\mathbf{A})$ is

$$\Pr(p \text{ divides } \det(\mathbf{A}))=1-\prod_{k=1}^{n}\left(1-p^{-k}\right),$$

if we assume that the integer entries are chosen so that each residue modulo p is equally likely.

To see this, let $\mathbf{A}^{\sim}$ be the matrix obtained by reducing each entry of $\mathbf{A}$ to its least nonnegative residue modulo p. Then $\det(\mathbf{A})$ is divisible by p if and only if $\mathbf{A}^{\sim}$ is singular as a matrix over the field $\mathbf{Z}_p$ of integers modulo p. There are

$$(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$$

invertible matrices among the p^{n^2} equally likely $n\times n$ matrices over $\mathbf{Z}_p$, so the probability that p divides $\det(\mathbf{A})$ is

$$1-\frac{(p^n-1)(p^n-p)\cdots(p^n-p^{n-1})}{p^{n^2}}.$$

A737. We show more generally by induction that if

$$Q_n(x)=1-\frac{x}{a_1}+\frac{x(x-a_1)}{a_1a_2}-\cdots+\frac{(-1)^n(x)(x-a_1)\cdots(x-a_{n-1})}{a_1a_2\cdots a_n}, \quad (1)$$

then

$$Q_n(x)=\frac{(a_1-x)(a_2-x)\cdots(a_n-x)}{a_1a_2\cdots a_n},$$

so that

$$P_n(x) = \frac{Q_n(x) - 1 + x/a_1}{x}$$

where $a_i = i^2$. Thus, $P_n(n^2) = 1 - 1/n^2$.

Assume (1) is valid for $n = k$. Then,

$$Q_{k+1}(x) = \frac{(a_1 - x)(a_2 - x)\cdots(a_k - x)}{a_1 a_2 \cdots a_k} + \frac{(-1)^{k+1}(x)(x - a_1)\cdots(x - a_k)}{a_1 a_2 \cdots a_{k+1}}$$
$$= \frac{(a_1 - x)(a_2 - x)\cdots(a_k - x)}{a_1 a_2 \cdots a_k}\left(1 - \frac{x}{a_{k+1}}\right).$$

Thus our result is also true for $n = k + 1$. Since the result also holds for $n = 1$, it holds for all n.

A738. Choose $g(x) = (f(-x))^r(f(x))^s$. Then $g(x)$ satisfies the requirements of Rolle's Theorem. Thus, there is a number $c \in (-1, 1)$ such that $-r(f(-c))^{r-1}f'(-c)(f(c))^s + s(f(-c))^r(f(c))^{s-1}f'(c) = 0$. Dividing by $(f(-c))^{r-1}(f(c))^{s-1}$ yields the desired result.

Complex Analysis for Beginners

Beginner I am, and ready to learn.
I'll listen, I'll study, an "A-plus" I'll earn!
But complex analysis, is it science or art?
There's this strange, peculiar, "imaginary" part.
Our professors who teach, to them it's quite clear
but to those of us learning, each solution comes dear.
And while many my questions, I never doubt
the wisdom of those who explored here about
this pure refined mind-stuff and left here behind
their names as the markers on discov'ries sublime:
Wessel and Schwarz, Christoffel, Laplace,
Rouché and Euler, Möbius, Lindelöf,
Cauchy and Riemann, Hamilton and Gauss,
Dirichlet, Cardano, Argand and Weierstrass.

Now with their aid I've begun my start,
fathoming depths of intellect and heart
those wisest of minds framed in formulas and laws,
small fragments of vastness, man's greatest "aha's."

—Kurt Kleinschnitz
P.O. Box 1691
Fairfield, IA 52556

so that

$$P_n(x) = \frac{Q_n(x) - 1 + x/a_1}{x}$$

where $a_i = i^2$. Thus, $P_n(n^2) = 1 - 1/n^2$.

Assume (1) is valid for $n = k$. Then,

$$Q_{k+1}(x) = \frac{(a_1 - x)(a_2 - x)\cdots(a_k - x)}{a_1 a_2 \cdots a_k} + \frac{(-1)^{k+1}(x)(x - a_1)\cdots(x - a_k)}{a_1 a_2 \cdots a_{k+1}}$$
$$= \frac{(a_1 - x)(a_2 - x)\cdots(a_k - x)}{a_1 a_2 \cdots a_k}\left(1 - \frac{x}{a_{k+1}}\right).$$

Thus our result is also true for $n = k + 1$. Since the result also holds for $n = 1$, it holds for all n.

A738. Choose $g(x) = (f(-x))^r(f(x))^s$. Then $g(x)$ satisfies the requirements of Rolle's Theorem. Thus, there is a number $c \in (-1, 1)$ such that $-r(f(-c))^{r-1}f'(-c)(f(c))^s + s(f(-c))^r(f(c))^{s-1}f'(c) = 0$. Dividing by $(f(-c))^{r-1}(f(c))^{s-1}$ yields the desired result.

Complex Analysis for Beginners

Beginner I am, and ready to learn.
I'll listen, I'll study, an "A-plus" I'll earn!
But complex analysis, is it science or art?
There's this strange, peculiar, "imaginary" part.
Our professors who teach, to them it's quite clear
but to those of us learning, each solution comes dear.
And while many my questions, I never doubt
the wisdom of those who explored here about
this pure refined mind-stuff and left here behind
their names as the markers on discov'ries sublime:
Wessel and Schwarz, Christoffel, Laplace,
Rouché and Euler, Möbius, Lindelöf,
Cauchy and Riemann, Hamilton and Gauss,
Dirichlet, Cardano, Argand and Weierstrass.

Now with their aid I've begun my start,
fathoming depths of intellect and heart
those wisest of minds framed in formulas and laws,
small fragments of vastness, man's greatest "aha's."

—Kurt Kleinschnitz
P.O. Box 1691
Fairfield, IA 52556

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.

Data compression: Prntg by nmbrs, *The Economist* (21 May 1988) 100-101.

The self-similarity of fractals affords extreme compression of data (particularly certain kinds of graphic images), but the cost in computation is high.

Department of Mathematics and Computer Science, North Carolina School of Science and Mathematics, *Geometric Probability*, NCTM, 1988; v + 40 pp + IBM-format diskette, $9 (P).

This is the first unit in a course being developed to prepare high-school students for the variety of math courses they may encounter in college. This unit presumes algebra II and geometry. It comes with a diskette (for IBM-compatible computers) with simulations of the experiments discussed in the text.

Steen, Lynn Arthur, The science of patterns, *Science* 240 (29 April 1988) 611-616.

"Mathematics is the science of patterns ... computers change not so much the nature of the discipline as the scale: computers are to mathematics what telescopes and microscopes are to science. They have increased by a millionfold the portfolio of patterns investigated by mathematical scientists. ... Because of computers, we see more than ever before that mathematical discovery is like scientific discovery." Steen celebrates the changes and growth in 20th-century mathematics growing into the mathematical sciences. He details recent discoveries in statistical science, core mathematics, and applied mathematics, in an essay we would be well advised to share with our colleagues in other fields, as well as our students.

Peterson, Ivars, Unknotting a tangled tale, *Science News* 133 (21 May 1988) 328-330.

Explains the newly-discovered polynomial invariants for knots, together with their applications to DNA coiling and connections with statistical mechanics.

Gleick, James, The quest for true randomness finally appears successful, *New York Times* (19 April 1988) 23-25.

Discusses randomness in general and a new technique for generating random numbers that arises from one-way functions. "The new technique involves taking some starting number, multiplying it by itself, dividing by the product of two primes, taking the remainder and using it to repeat the process over and over again ... [T]here is a peculiar connection between the randomness of the outcome and the difficulty of factoring large numbers ... [I]f factoring large numbers is truly hard ... the resulting sequence will be indistinguishable from true randomness." The new technique is the work of S. Micali (MIT) and others.

Rubik, Ernő, et al., *Rubik's Cubic Compendium*, Oxford Univ. Pr., 1988; xi + 225 pp, $26.95.

The history and the art of Rubik's cube, in an excellent little book with many color illustrations.

Rubik's Magic Strategy Game, Matchbox, 1987; $9.95.

Tic-tac-toe on a 4×4 board, with some ingenious complications. I will be disappointed if we do not see some mathematical analyses of this game: Is a draw possible? Is there a winning strategy for one player or the other? Is there a succinct winning strategy?

"Hot hands" phenomenon: A myth?, *New York Times* (19 April 1988) 23, 25.

Most basketball coaches and fans believe that a player who has made a string of baskets is more likely to succeed in the next try. But an exhaustive study by psychologist A. Iversky (Stanford), examining thousands of shots in actual games (of the Philadelphia 76ers over a season and a half), has found otherwise: Outcomes of successive shots are independent. No doubt students will be interested in this example of statistical independence, but will they really give up their belief in "hot hands"?

Chaitin, Gregory J., Randomness in arithmetic, *Scientific American* 256:7 (July 1988) 80-85. Beyond Gödel's proof, *Research* (IBM Research Magazine) 25:8 (Fall 1987) 12-15.

Gregory Chaitin (IBM Watson Research Center) has shown that there can be no proof that a string of digits is random. His result is a kind of incompleteness theorem, "a dramatic extension of Gödel's work" (Martin Davis). Chaitin has produced a diophantine equation with 17,000 variables and an integer parameter K. He asks for each K, does the equation have a finite number of solutions or an infinite number? The sequence of answers forms a binary string whose information content cannot be compressed (because the answers are independent) and which is consequently a truly random number. The randomness of the answers means that "there are an infinite number of mathematical facts that cannot be connected by mathematical deduction with any formal axiomatic system." Put bluntly, randomness and unpredictability lie unavoidably at the heart of mathematics.

Boyd, James N., *Professor Bear's Mathematical World*, Virginia Council of Teachers of Mathematics, 1987; 120 pp (P).

Delightful collection of cartoons, many of them based on bearly bearable puns ("plane and sordid geometry," "bearnary mathematics,", "bearloney," "Professor LoBEARchevsky meets BEARnhard Riemann"—you get the idea).

Klamkin, Murray S., *International Mathematical Olympiads* 1979-1985 *and Forty Supplementary Problems*, MAA, 1986; xii + 141 pp, $11.50.

In this problem collection Murray Klamkin includes as a bonus 40 additional problems that were submitted to the Olympiad Committee but not used. Readers keen on problem-solving can find problems from other nations's competitions in his column in *Crux Mathematicorum*.

Miyazaki, Koji, *An Adventure in Multidimensional Space: The Art and Geometry of Polygons, Polyhedra, and Polytopes*, Wiley, 1986; vi + 112 pp, $49.95.

A visual feast of shape and geometry. Unlike other works on polygons and polyhedra, this book shows many illustrations (many in color) from Eastern art and architecture.

Romano, Joseph P., and Andrew F. Siegel, *Counterexamples in Probability and Statistics*, Wadsworth & Brooks/Cole, 1986; xxiv + 303 pp., $34.95.

Long overdue, at last there is a reference collection of 300+ counterexamples in probability and statistics. Work on this volume was begun by the "senior" author as an undergraduate; it's too bad we can't count on more senior professionals to compile such useful handbooks.

Hargittai, István, and Magdolna Hargittai, *Symmetry through the Eyes of a Chemist*, VCH Publishers, 1986; vii + 458 pp, $95.00.

"This relatively short book surveys the entire field of chemistry from the point of view of symmetry." Topics include molecular vibrations, electronic structure of atoms and molecules, chemical reactions, space-group symmetries, and symmetries in crystals.

The Spode Group, *Motivating A-Level Mathematics: A Source Book*, Oxford University Press, 1986; ix + 130 pp, $24.95.

Case studies illustrating many applications of topics from the British A-level examination by Clabus: functions, calculus, mechanics, and probability and statistics. (Unfortunately, "Art Forgeries" seems to have been adapted from a well-known source without acknowledgment.)

NEWS AND LETTERS

LETTERS TO THE EDITOR

Dear Editor:

Since n and $2n$-1 are relatively prime, and since $\binom{2n}{n}$ is even, it follows from

$$\binom{2n-2}{n-1} = \binom{2n}{n}\frac{n}{2(2n-1)}$$

that $\binom{2n-2}{n-1}$ is divisible by n. $\binom{2n}{n}$ is even because

$$\binom{2n}{n} = 2^{2n} - 2\left[\binom{2n}{0} + \dots + \binom{2n}{n-1}\right].$$

Note: If n is odd, then it is sufficient to note that n and $2(2n - 1)$ are relatively prime.

Lajos Takács
Case Western Reserve University

[Ed. Note: Professor Takács also provided the proof given below by Richard Guy.]

Dear Editor:

I'm astonished to see the names of four well-known mathematicians in the context of p. 207 of the current *Math. Mag.*

$$\frac{(2n-2)!}{n!(n-1)!} = \frac{(2n-2)!}{n!(n-1)!}[2n - (2n-1)]$$

$$= 2\binom{2n-2}{n-1} - \binom{2n-1}{n-1}$$

or

$$= \frac{(2n-2)!}{n!(n-1)!}[n - (n-1)] = \binom{2n-2}{n-1} - \binom{2n-2}{n-2}$$

each of which is an integer. This is as elementary a proof as you can get, since one needs to know what a binomial coefficient is: the only other fact is that it's an integer!

Richard K. Guy
University of Calgary

[Ed. Note: The same proof was provided by Ira Gessel, Colin Wilson, and Barry Wolk.]

Dear Editor:

We are hoist on our own pétard.

Joel Brenner
Palo Alto, CA

Dear Editor:

Will the following proof end the debate?

$$\binom{2n-1}{n} = \frac{2n-1}{n}\binom{2n-2}{n-1}.$$

Since n is coprime to $2n - 1$, n divides $\binom{2n-2}{n-1}$.

R.J. Clarke
The University of Adelaide

[A slight variant of this was given by R.K. Bruynel.]

Dear Editor:

In the excellent article, "The Ubiquitous Pi," in the April issue of Mathematics Magazine, appears a misleading statement. On page 68, one reads: "The Hindu mathematician Brahmagupta was led astray by the fact that the perimeters of polygons of 12, 24, 48, and 96 sides inscribed in a circle with diameter 10 are *given by* $\sqrt{965}$, $\sqrt{981}$, $\sqrt{986}$, and $\sqrt{987}$." This wording suggests to me that they are the exact values for these perimeters but such is not the case. For example, the exact value of the perimeter of the dodecagon is $60\sqrt{2 - \sqrt{3}} \neq \sqrt{965}$.

John P. Hoyt
Lancaster, PA

Dear Editor:

"The Ubiquitous Pi" has caught the fancy of many of us. However, I have a question.

In the June 1988 issue of *Mathematics Magazine*, Dario Castellanos states that the largest known prime—a Mersenne prime—is the number reported there, a number of 39,751 digits. However, in the summer of 1985, it was announced that a still larger Mersenne prime had been found, a number of 65,050 digits; to wit

$$2^{216,091} - 1$$

—which, of course, provides a lagniappe in generating the largest known perfect number as well.

Michael W. Ecker
Pennsylvania State University
Wilkes-Barre Campus

Dear Editor:

Readers who constructed the tetrahedron described by Rick Norwood on pages 101-102 of the April 1988 issue may be interested to know that it is also possible to *braid* together

2 US bills to form a regular tetrahedron,
3 US bills to form a regular hexahedron (cube),
and 4 US bills to form a regular octahedron.

Since US bills are all of the same size (try other currencies to see how special this property is!) any denomination you can afford will work. The important point, however, is that in each case the construction may be done so that the model

(i) has every face and every edge covered by at least one of the bills,

(ii) shows an equal area from each bill,

(iii) has no loose ends protruding from its surface,

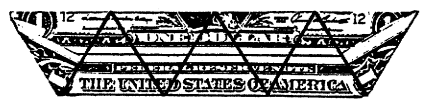
and

(iv) requires no paper clips, or other fastening devices to make it stable.

The illustration below shows one way that dollar bills may be folded to make these models (readers may wish to experiment with variations in order to get their favorite part of the bill to appear on the finished model). The bill in Figure (a) was folded precisely as described by Norwood. The bills in Figures (b) and (c) were first folded in half lengthwise, and then, with that initial fold line as a guide, the long edges were folded in to meet the center line. The fold lines for the three center squares of Figure (b) were determined by placing two folded bills over each other at right angles. The right and left hand rectangles cannot both be squares (just make certain they are of about equal size—then one end may be fitted inside the other and the overlapping arrangement adjusted to form the required square). The triangles of Figure (c) were folded as described by Norwood.

(a) Two of these make a regular tetrahedron

(b) Three of these make a regular hexahedron (cube)



(c) Four of these make a regular octahedron

I don't want to spoil the reader's fun by saying anything more about how to construct these models but, to insure against unnecessary frustration, I include the following references, any one of which would provide ample detail.

REFERENCES

[1] Martin Gardner, Mathematical Games: The plaiting of Plato's polyhedrons and the assymmetrical ying-yang-lee, *Scientific American*, September, 1971, 204-212.

[2] Jean Pedersen, Plaited platonic puzzles, *Two Year College Math. J.* 5 (1974) 22-37.

[3] Peter Hilton and Jean Pedersen, *Build Your own Polyhedra*, Addison-Wesley Publishing Co., 1988, pp. 93-98.

Jean Pedersen
Santa Clara University

"There was more imagination in the head of Archimedes than in that of Homer."—Voltaire

And there's more imagination, astonishment, and wit in the pages of *Archimedes' Revenge* than in any number of other books about mathematics.

"Other works have rhapsodized at length about the nature of infinity and the beauty of 'higher dimensions'," says the author, Paul Hoffman. "Such philosophical excursions have their place, but are far from the concerns of most working mathematicians. I give a glimpse here of some of the other things that mathematicians, pure and applied, actually do."

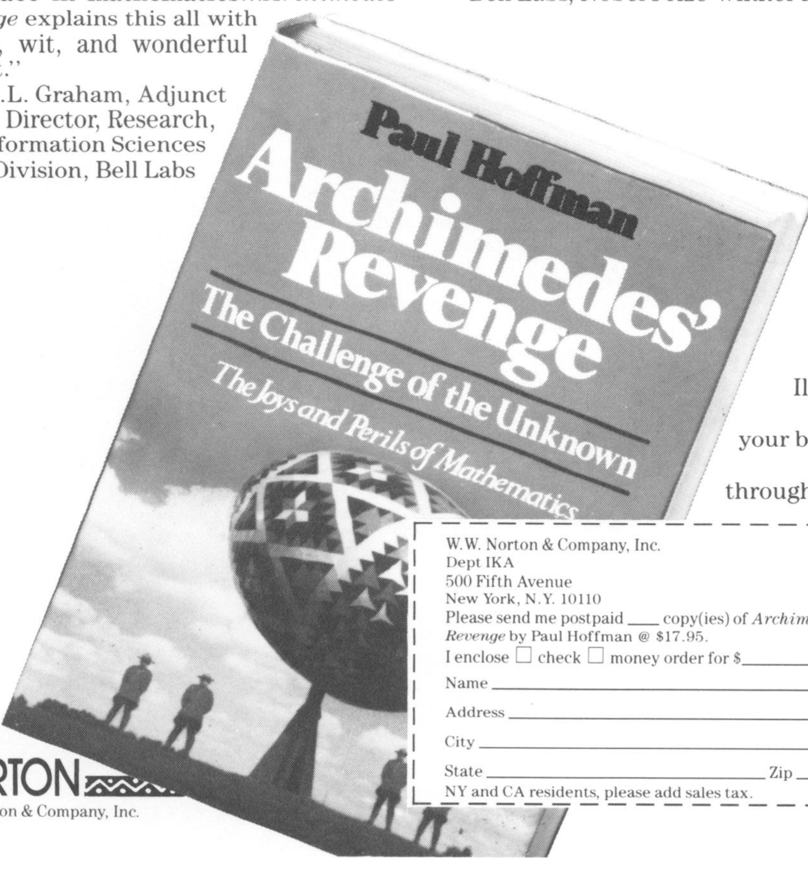
"**Paul Hoffman gives us a rare view into some of the profound changes now taking place in mathematics**...*Archimedes' Revenge* explains this all with clarity, wit, and wonderful insight."
—R.L. Graham, Adjunct Director, Research, Information Sciences Division, Bell Labs

"**Students of recreational mathematics will be delighted** with this new collection of exciting problems, paradoxes, brain teasers and curiosities." —Martin Gardner

"**Engaging, highly readable...**Algorithms, geometric theory, perfect numbers, and a quantum approach to congressional representation are a few of the topics explored." —*Booklist*

"**Fascinating.**" —Isaac Asimov

"**Informative and entertaining.**"
—Arno Penzias, Vice President of Research, Bell Labs, Nobel Prize-winner in Physics



Illustrated. Now at your bookstore, or order through coupon.

W.W. Norton & Company, Inc.
Dept IKA
500 Fifth Avenue
New York, N.Y. 10110
Please send me postpaid ____ copy(ies) of *Archimedes' Revenge* by Paul Hoffman @ $17.95.
I enclose ☐ check ☐ money order for $________
Name ________
Address ________
City ________
State ________ Zip ________
NY and CA residents, please add sales tax.

NORTON
W.W. Norton & Company, Inc.

CONTENTS

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