PI MU EPSILON JOURNAL

VOLUME 8 SPRING 1986 NUMBER 4

CONTENTS

PI MU EPSILON JOURNAL

VOLUME 8 SPRING 1986 NUMBER 4

CONTENTS

PI MU EPSILON JOURNAL
THE OFFICIAL PUBLICATION
OF THE HONORARY MATHEMATICAL FRATERNITY

Joseph D.E. Konhauser, Editor

ASSOCIATE EDITOR
Clayton W. Dodge

OFFICERS OF THE FRATERNITY
President: Milton D. Cox, Miami University
President-Elect: Eileen L. Poiani, Saint Peter's College
Secretary-Treasurer: Richard A. Good, University of Maryland
Past-President: E. Maurice Beesley, University of Nevada

COUNCILORS
David W. Ballew, South Dakota School of Mines and Technology
Robert C. Eslinger, Hendrix College
Virginia Taylor, University of Lowell
Robert M. Woodside, East Carolina University

Editorial correspondence, including books for review, chapter reports, news items and manuscripts (two copies) should be mailed to EDITOR, PI MU EPSILON JOURNAL, Mathematics and Computer Science Department, Macalester College, St. Paul, MN 55105. Students submitting manuscripts are requested to identify their college or university and their class or expected graduation date. Others are requested to provide their affiliation, academic or otherwise.

Problems for solution and solutions to problems should be mailed directly to the PROBLEM EDITOR. Puzzle proposals and puzzle solutions should be mailed to the EDITOR.

The PI MU EPSILON JOURNAL is published at Macalester College twice a year—Fall and Spring. One volume consists of five years (10 issues) beginning with the Fall 19x4 or Fall 19x9 issue, starting in 1949. For rates, see inside back cover.

OF EXOTIC INTEGERS AND QUATERNIONS -- AN INTRODUCTION TO REPRESENTATION THEORY.

by Thomas Dick
University of New Hampshire

One's first encounter with complex numbers is usually undertaken with a little mistrust in their legitimacy. After all, any objects with "imaginary" parts do not beg to be taken too seriously. However, if we suspend our disbelief at the thought of a square root of -1, we are soon happily computing with complex numbers as easily as we would with real numbers. The lofty praise given to the algebraic closure of the complex numbers (that is, the fact that any polynomial with complex coefficients will have a complex root) is taken with a grain of salt, since we invented solutions to the equation $x^2 + 1 = 0$ in the first place.

After repeated exposure to the topic of complex numbers our protests tend to die down. Some of us are reassured by an alternative description of complex numbers which avoids any mention of the bizarre "i" = $(\sqrt{-1})$. We can identify, or equivalently, define complex numbers as ordered pairs (a,b) of real numbers. The addition of these ordered pairs is defined "coordinate-wise":

$$(a,b) + (c,d) = (a + c, b + d).$$

The multiplication of ordered pairs is defined in a slightly more involved way:

$$(a,b)(c,d) = (ac - bd, ad + bc).$$

This multiplication appears somewhat contrived. Indeed, this definition of the complex numbers simply reflects our desire to have a square root of -1. For, if we identify i with $(0,1)$ and -1 with $(-1,0)$, we have

$$i^2 \text{ "=" } (0,1)(0,1) = (-1,0) \text{ "=" } -1.$$

It is straightforward to verify that the ordered pair (a,b) behaves exactly like the complex number $a + bi$. It might be said that we have successfully "represented" complex numbers as ordered pairs of real numbers.

There does exist yet another representation of the complex

PI MU EPSILON JOURNAL
THE OFFICIAL PUBLICATION
OF THE HONORARY MATHEMATICAL FRATERNITY

Joseph D.E. Konhauser, Editor

ASSOCIATE EDITOR
Clayton W. Dodge

OFFICERS OF THE FRATERNITY
President: Milton D. Cox, Miami University
President-Elect: Eileen L. Poiani, Saint Peter's College
Secretary-Treasurer: Richard A. Good, University of Maryland
Past-President: E. Maurice Beesley, University of Nevada

COUNCILORS
David W. Ballew, South Dakota School of Mines and Technology
Robert C. Eslinger, Hendrix College
Virginia Taylor, University of Lowell
Robert M. Woodside, East Carolina University

Editorial correspondence, including books for review, chapter reports, news items and manuscripts (two copies) should be mailed to EDITOR, PI MU EPSILON JOURNAL, Mathematics and Computer Science Department, Macalester College, St. Paul, MN 55105. Students submitting manuscripts are requested to identify their college or university and their class or expected graduation date. Others are requested to provide their affiliation, academic or otherwise.

Problems for solution and solutions to problems should be mailed directly to the PROBLEM EDITOR. Puzzle proposals and puzzle solutions should be mailed to the EDITOR.

The **PI MU EPSILON JOURNAL** is published at Macalester College twice a year—Fall and Spring. One volume consists of five years (10 issues) beginning with the Fall 19x4 or Fall 19x9 issue, starting in 1949. For rates, see inside back cover.

OF EXOTIC INTEGERS AND QUATERNIONS -- AN INTRODUCTION TO REPRESENTATION THEORY

by Thomas Dick
University of New Hampshire

One's first encounter with complex numbers is usually undertaken with a little mistrust in their legitimacy. After all, any objects with "imaginary" parts do not beg to be taken too seriously. However, if we suspend our disbelief at the thought of a square root of -1, we are soon happily computing with complex numbers as easily as we would with real numbers. The lofty praise given to the algebraic closure of the complex numbers (that is, the fact that any polynomial with complex coefficients will have a complex root) is taken with a grain of salt, since we invented solutions to the equation $x^2 + 1 = 0$ in the first place.

After repeated exposure to the topic of complex numbers our protests tend to die down. Some of us are reassured by an alternative description of complex numbers which avoids any mention of the bizarre "$i = (\sqrt{-1})$". We can identify, or equivalently, define complex numbers as ordered pairs (a,b) of real numbers. The addition of these ordered pairs is defined "coordinate-wise":

$$(a,b) + (c,d) = (a + c, b + d).$$

The multiplication of ordered pairs is defined in a slightly more involved way:

$$(a,b)(c,d) = (ac - bd, ad + bc).$$

This multiplication appears somewhat contrived. Indeed, this definition of the complex numbers simply reflects our desire to have a square root of -1. For, if we identify i with $(0,1)$ and -1 with $(-1,0)$, we have

$$i^2 = (0,1)(0,1) = (-1,0) = -1.$$

It is straightforward to verify that the ordered pair (a,b) behaves exactly like the complex number $a + bi$. It might be said that we have successfully "represented" complex numbers as ordered pairs of real numbers.

There does exist yet another representation of the complex

numbers - as certain 2x2 real matrices. Specifically, the complex number a + bi is represented by the 2x2 square array of real numbers $\begin{pmatrix} a. \\ -b. \end{pmatrix}$ It is this type of representation that is the subject of this article. Not only can the complex numbers be represented in such a manner, but also many other "strange" number systems, such as Gaussian, hyperbolic, and parabolic integers, as well as the quaternions. The idea of representing the objects of an algebraic system as matrices has proven to be one of the most powerful and fruitful ideas in all mathematics. So-called ***representation theory*** remains an active area of research that arises in many different branches and contexts of mathematics. It is our purpose to provide an introduction to representation theory by way of illustrating how several seemingly quite different number systems can all be represented by 2x2 matrices. First, for the sake of completeness, we provide a brief review of the algebra of such matrices.

Algebra of 2x2 matrices. A 2x2 matrix is simply a square array of numbers of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If the entries a, b, c, and d are all integers, we call this an integral matrix. Similarly, if all of the entries are real or complex numbers, we call the matrix real or complex, respectively. The addition of two 2x2 matrices is accomplished "entry-wise":

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ c+c' & d+d' \end{pmatrix},$$

while the product of two 2x2 matrices is defined by the formula:

$$\begin{pmatrix} b \\ d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}$$

With these two operations, the set of all 2x2 integral (or real or complex) matricesbecomesa ***ring**.* That is, if A, B, and C are any 2x2 integral (or real or complex) matrices, and if we let

$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ d $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, then the following properties hold:

* Strictly speaking, we should speak of an ***associative ring with identity,*** since the term "ring" is also used in contexts where associativity of multiplication or existence of a multiplicative identity are not assumed.

1). A + (B + C) = (A + B) + C
2). A + B = B + A
3). A + 0 = 0 + A = A
4). A + (-A) = (-A) + A = 0 (where -A denotes the matrix whose entries* are the additive inverses of the entries of A).
5). A(BC) = (AB)C
6) AI = IA = A
7) A(B + C) = AB + AC, (A + B)C = AC + BC

A couple of observations are in order. First, matrix multiplication is generally not commutative, as can be seen from the fact that

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \text{ while } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Secondly, a nonzero matrix need not have a multiplicative inverse. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we define. the ***determinant*** of A to be det(A) = ad - bc. If det(A) # 0, then the matrix

$$A^{-1} = \begin{pmatrix} \frac{d}{ad - bc} & \frac{-b}{ad - bc} \\ \frac{-c}{ad - bc} & \frac{a}{ad - bc} \end{pmatrix}$$

has the property that $AA^{-1} = A^{-1}A = I$. Even if ad - bc ≠ 0, the matrix A may not have an inverse. For example, if we restrict ourselves to considering integral matrices, we see that A^{-1} is not necessarily an integral matrix itself.

Matrices may also be multiplied by scalars (numbers) by distributing the multiplication across all entries. Hence, $s \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} sb \\ sd \end{pmatrix}$. This scalar multiplication satsifies two distributive laws:

1). s(A + B) = sA + sB 2). (s + t)A = sA + tA

for all scalars s, t and matrices A, B.# With scalar multiplication defined, we may note that -A = (-1)A.

With the scalar multiplication defined here we sometimes refer to the ring of matrices as an algebra, especially in the case that the scalars come from a field like the set of real numbers or the set of complex numbers.

Basics of Representation Theory. We will adopt the common notation of $\mathbb{Z}$ for the set of integers, $\mathbb{R}$ for the set of real numbers and $\mathbb{C}$ for the set of complex numbers. The set of all 2x2 matrices with integral entries will be denoted $M_2(\mathbb{Z})$. Similarly, the set of all 2x2 real matrices and the set of all 2x2 complex matrices will be denoted $M_2(\mathbb{R})$ and $M_2(\mathbb{C})$, respectively. As indicated before, with the usual addition and multiplication of matrices, each of these sets is a ring.

Now, suppose that N is a number system. By this we simply mean that N is some set of elements with an addition (+) and multiplication (·) defined on it. We will not suppose that the addition and multiplication of N obey any particularly nice or familiar laws. Indeed, we will want to examine some number systems with quite strange properties. In order to carry out an investigation of a number system N, we will represent the elements of N as certain matrices. But not any such representation will be useful. We will want the addition and multiplication of N to "carry over" to the usual addition and multiplication of matrices. Let us make this notion very precise with the following definitions:

> A number system N has an ***integral representation*** as 2x2 matrices if we can assign to each element x belonging to N a 2x2 integral matrix $M(x)$ such that the following properties hold for all x, y in N:
>
> i). $M(x + y) = M(x) + M(y)$
>
> ii). $M(xy) = M(x)M(y)$
>
> We say that N has a ***real representation*** or ***complex representation*** as 2x2 matrices if the matrix $M(x)$ is a 2x2 real or complex matrix, respectively, for each x in N. In any of these cases, we refer to the function which assigns $M(x)$ to x as a ***representation*** of N.

In other words, a representation of N is simply a function from N to some set of matrices which always "respects" the addition and multiplication of elements of N.

We have purposely avoided as much of the terminology of abstract algebra as possible. For the reader who has an acquaintance with a little ring theory we point out that if N itself is a ring, then a representation of N is just a ring homomorphism from N to a particular matrix ring.

Examples. 1. Every number system N has an integral (as well as a real and complex) representation as 2x2 matrices, although it is not very interesting. The ***trivial*** representation of N is obtained by assigning the zero matrix $\begin{pmatrix} 0 & \\ 0 & \end{pmatrix}$ to each element of N. That is, for every x ∈ N, $M(x) = 0$. The required properties, i). $M(x + y) = M(x) + M(y)$ and ii). $M(xy) = M(x)M(y)$, are certainly satisfied in this case, as all matrices considered are zero matrices.

2. As mentioned in the introduction, the complex numbers can be represented as 2x2 real matrices via the function $M(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. It remains to be seen whether or not this is a real representation according to the mathematical definition discussed above. To verify that this is indeed a real representation, we must check that the two properties hold with $M(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, and $M(c + di) = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ for any two complex numbers $(a + bi)$ and $(c + di)$. Since i). $M(a + bi) + M(c + di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = M((a+c) + (b+d)i)$, and ii). $M(a + bi)M(c + di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} = M((ac-bd) + (ad+bc)i)$, we see that this assignment of matrices actually is a real representation of the complex numbers. (One observation concerning this representation merits some attention. The determinant of the matrix representative of a complex number $a + bi$ turns out to be its squared distance from the origin when considered as an ordered pair (a,b) of real numbers.)

Example 2 also serves as an illustration of a ***faithful*** representation. A faithful representation is one which establishes a one-to-one correspondence between the number system N and some set of matrices. Precisely, a representation is faithful if and only if $M(x) = M(y)$ implies $x = y$ for any x and y in N. In example 2, since $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ if and only if $a = c$ and $b = d$, we have $M(a + bi) = M(c + di)$ if and only if $a + bi = c + di$. In ring theoretic terminology, a faithful representation establishes an isomorphism between a ring N and a particular ring of matrices.

3. Faithful representations of $\mathbb{Z}$, R, and $\mathbb{C}$ as 2x2 integral, real, and complex matrices, respectively, can be realized using the *scalar* representation:

$$M(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \quad \text{for } a \text{ in } \mathbb{Z} \text{ or R or C.}$$

We verify that this is a representation by noting

i). $M(a) + M(b) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix} = M(a + b)$, and

ii). $M(a)M(b) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} = M(ab)$. The scalar representation is faithful, since $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}$ implies a = b.

Faithful representations are the most important kinds of representations, as they provide us with a "clone" (i.e., isomorphic copy) of the number system under study as a set of matrices. Why is this desirable? We give three primary reasons:

i). The elements of an unfamiliar number system can be made more "concrete" by representing them as matrices with more familiar entries. In example 2 above, we represented complex numbers with matrices which had real entries.

ii). Different number systems can be compared in a common setting. If two number systems can both be represented as 2x2 integral matrices, for example, then we can more easily recognize the essential similarities and differences between the two systems.

iii). Once a number system has been faithfully represented, we have all the powerful tools of matrix theory at our disposal for investigating the system. For example, the existence of multiplicative inverses is easy to check by using the determinant as a criterion.

We will now proceed to examine a few "exotic" number systems by utilizing faithful representations of them. A final comment before we begin -- if we adopt the usual convention of considering $\mathbb{R}$ as a subset of $\mathbb{C}$, and if we consider $\mathbb{Z}$ as a subset of $\mathbb{R}$, then any integral representation is automatically a real representation, and a real representation is automatically a complex representation.

Gaussian Integers. The set of Gaussian integers, which we will denote as G, can best be thought of as the set of all complex numbers with integral real and imaginary parts. That is, $G = \{m + ni \in \mathbb{C}: m, n \in \mathbb{Z}\}$.

Examples of Gaussian integers would include $2 + 3i$, 17, $-6i$, and $-4 + 5i$. The Gaussian integers inherit a faithful representation as 2x2 integral matrices simply by using the real representation for $\mathbb{C}$ discussed above and restricting it to G. In other words,

$$M(m + ni) = \begin{pmatrix} m & n \\ -n & m \end{pmatrix}$$

gives us a faithful representation of G as 2x2 integral matrices. That G is a ring is easy to verify, and the multiplication in G is commutative. However, elements of G do not generally have multiplicative inverses. Here we can make use of our representation to find exactly which elements of G have multiplicative inverses. Since our representation is faithful, a Gaussian integer $g = m + ni$ will have a multiplicative inverse if and only if its matrix representative $\begin{pmatrix} m \\ -n \end{pmatrix}$ has an inverse which is the representative of a Gaussian integer. To see this, note that if g has an inverse g^{-1}, then we have

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = M(1) = M(gg^{-1}) = M(g)M(g^{-1}), \text{ i.e., } M(g^{-1}) = M(g)^{-1}.$$

Since $g = m + ni$, we have $M(g) = \begin{pmatrix} m \\ -n \end{pmatrix}$, and the inverse of M(g) must be

$$M(g)^{-1} = \begin{pmatrix} \frac{m}{m^2+n^2} & \frac{-n}{m^2+n^2} \\ \frac{n}{m^2+n^2} & \frac{m}{m^2+n^2} \end{pmatrix}$$

For this to be the representative of a Gaussian integer, all of its entries must be integers, or equivalently, the integer $m^2 + n^2$ must divide each of the integers m and n. A little reflection convinces us that this can only happen in the case that $m = \pm 1$ or -1, $n = 0$, or in the case $n = +1$ or -1, $m = 0$. Thus, the only Gaussian integers which have multiplicative inverses within the system of Gaussian integers are: 1, -1, i, -i.

Parabolic Integers. Formally, the set of parabolic integers, which we will denote as P, is

$$P = \{m + nj: m, n \in \mathbb{Z}, j^2 = 0, j \neq 0\}.$$

The element j is certainly not a number within our usual realm of experience, since j is nonzero, yet j^2 is zero. But the imaginary number i was no less strange at first glance, and this j seems no more

artificial and contrived than a square root of -1. Even though j is outside the system of complex numbers, we can find a faithful 2x2 integral representation for P just as we did for the Gaussian integers G. The secret, of course, will be finding a suitable matrix representative for j.

The addition and multiplication in P is analogous to that of the complex numbers -- we add and multiply two parabolic integers as if they were binomials, and then simplify the expression using the formal identity $j^2 = 0$. As an example.

$$(2 - 3j) + (-4 + 2j) = (-2 - j),$$

while $(2 - 3j)(-4 + 2j) = -8 + 4j + 12j - 6j^2 = -8 + 16j + 0 = (-8 + 16j)$.

A faithful representation of P as 2x2 integral matrices is given by

$$M(m + nj) = \begin{pmatrix} m & n \\ 0 & m \end{pmatrix},$$

We verify that this indeed gives us a representation of P by noting that

$$M(m + nj) + M(m' + n'j) = \begin{pmatrix} m & n \\ 0 & m \end{pmatrix} + \begin{pmatrix} m' & n' \\ 0 & m' \end{pmatrix} = \begin{pmatrix} m+m' & n+n' \\ 0 & m+m' \end{pmatrix} =$$

$$M((m+m') + (n+n')j),$$

and $M(m + nj)M(m' + n'j) = \begin{pmatrix} m & n \\ 0 & m \end{pmatrix}\begin{pmatrix} m' & n' \\ 0 & m' \end{pmatrix} = \begin{pmatrix} mm' & mn'+nm' \\ 0 & mm' \end{pmatrix} =$

$M(mm' + (mn'+nm')j)$.

The representation is faithful, since $\begin{pmatrix} m & n \\ 0 & m \end{pmatrix} = \begin{pmatrix} m' & n' \\ 0 & m' \end{pmatrix}$ implies $m = m'$, $n = n'$. We note, in particular, that the parabolic integer j has matrix representative $M(j) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. We also note that any integer $s \in \mathbb{Z}$ can also be considered as a Gaussian integer (with zero imaginary part) or as a parabolic integer (with zero "j" part). In fact, we have $\mathbb{Z} = G \cap P$. The particular representations we have chosen for G and P reflect this, as the matrix representative of an integer s in either case is the scalar matrix $M(s) = \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix}$. We might say that our representations are "compatible" with respect to the integers.

Again, it is straightforward to verify that P is a commutative ring. P is not a field, but there are infinitely many elements of P which have multiplicative inverses in P. Just as with G, we see this by making use of the faithfulness of our representation and noting that the inverse of a matrix $M = \begin{pmatrix} m & n \\ 0 & m \end{pmatrix}$ is of the form $M^{-1} = \begin{pmatrix} 1/m & -n/m^2 \\ 0 & 1/m \end{pmatrix}$. Thus, M^{-1} is the representative of a parabolic integer precisely when $m = 1$ or $m = -1$. This shows that any parabolic integer of the form $(1 + nj)$ or $(-1 + nj)$, where n is any integer, has a multiplicative inverse. This inverse is the "conjugate", i.e., $(1 - nj)$ or $(-1 - nj)$, respectively.

Hyperbolic Integers. We next visit the hyperbolic integers, the set of which we will denote as H. Formally, $H = \{ m + nk: m, n \in \mathbb{Z}, k^2 = 1, k \neq 1 \text{ and } k \neq -1\}$. The number k is another number outside our usual acquaintances, and finding a suitable matrix representative for k will be the key to finding a representation of H. The addition and multiplication in H is accomplished in the same binomial fashion as in G and P. Thus, we have for any two hyperbolic integers $(m + nk)$, $(m' + n'k)$:

$$(m + nk) + (m' + n'k) = ((m + m') + (n + n')k),$$

and $$(m + nk)(m' + n'k) = ((mm' + nn') + (mn' + m'n)k).$$

Our representation of H is given by $M(m + nk) = \begin{pmatrix} m & n \\ n & m \end{pmatrix}$. To verify that this gives us a representation of the hyperbolic integers as 2x2 integral matrices we note:

$$M(m + nk) + M(m' + n'k) = \begin{pmatrix} m & n \\ n & m \end{pmatrix} + \begin{pmatrix} m' & n' \\ n' & m' \end{pmatrix} = \begin{pmatrix} m+m' & n+n' \\ n+n' & m+m' \end{pmatrix} =$$

$M((m+m') + (n+n')k)$

and $M(m + nk)M(m' + n'k) = \begin{pmatrix} m & n \\ n & m \end{pmatrix}\begin{pmatrix} m' & n' \\ n' & m' \end{pmatrix} = \begin{pmatrix} mm'+nn' & mn'+m'n \\ mn'+m'n & mm'+nn' \end{pmatrix} =$

$M((mm'+nn') + (mn'+m'n)k)$.

The representation is faithful since $\begin{pmatrix} m & n \\ n & m \end{pmatrix} = \begin{pmatrix} m' & n' \\ n' & m' \end{pmatrix}$ implies $m = m'$, $n = n'$.

As was the case with Gaussian and parabolic integers, the set of hyperbolic integers with their described addition and multiplication is a commutative ring. An analysis of matrix inverses reveals which elements of H have multiplicative inverses. The inverse of the matrix $M = \begin{pmatrix} m & n \\ n & m \end{pmatrix}$ is of the form

$$M^{-1} = \begin{pmatrix} \frac{m}{m^2 - n^2} & \frac{-n}{m^2 - n^2} \\ \frac{-n}{m^2 - n^2} & \frac{m}{m^2 - n^2} \end{pmatrix}.$$

m - n m - n

The reader can verify that we have a case similar to the one we had with the Gaussian integers, in the sense that M^{-1} will be a hyperbolic integer representative itself only if $m = \pm 1$, $n = 0$, or if $n = \pm 1$, $m = 0$. Thus, the only hyperbolic integers with multiplicative inverses are ± 1 and $\pm k$.

This representation of the hyperbolic integers is compatible with both of our previous representations of G and P with respect to the integers. In fact, we have $\mathbb{Z} = G \cap P = G \cap H = P \cap H = G \cap PDH$, and the integers are represented as scalar matrices in all our representations. A natural question which arises concerns how "much" of $M_2(\mathbb{Z})$ is accounted for by G, H and P. Before any reasonable answer to this question can be formulated, some clarification is required. First, since all three representations have equal entries along the main diagonal, any sum of Gaussian, hyperbolic and parabolic integer representatives will also have equal entries along the main diagonal. We certainly can't get just any 2x2 integral matrix in such a manner. However, if we also consider products of Gaussian, hyperbolic and parabolic integers, then any 2x2 integral matrix can be expressed as a sum of such products. To see this, we note that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = aJK + (b - c)J + cK + dKJ$, where J is the matrix representative of the parabolic integer j and K is the matrix representative of the hyperbolic integer k. (We've actually shown that P and H alone "generate" all 2x2 integral matrices, so certainly G, P and H will also. Will any other two of G, H and P generate all 2x2 integral matrices?)

Quaternions. At one time quaternions competed with vectors for mathematicians' favor as the desired model for a variety of physical phenomena. While Hamilton's invention eventually lost out, quaternions still provide us with a rich source of examples regarding "skew" fields, i.e., number systems with multiplicative inverses for their nonzero elements, but with a non-commutative multiplication.

Formally, a quaternion is of the form $q = a + bi' + cj' + dk'$, where the a, b, c and d are real numbers, and i', j', and k' are

nonreal entities whose behavior is best summarized by their multiplication table:

(first factor) \ (second factor) ·	i'	j'	k'
i'	-1	k'	-j'
j'	-k'	-1	i
k'	j'	-i'	-1

As can be seen, each of i', j' and k' is like the imaginary number i in the sense that $(i')^2 = (j')^2 = (k')^2 = -1$. We should take special note of the fact that the multiplication is definitely not commutative, as evidenced by $i'j' = k' = -j'i'$; $j'k' = i' = -k'j'$; and $k'i' = j' = -i'k'$. Two quaternions are added or multipled just like polynomials (real numbers do commute with i', j' and k') with the above multiplication table used to simplify products. Thus $(a+bi'+cj'+dk') + (w+xi'+yj'+zk') = (a+w) + (b+x)i' + (c+y)j' + (d+z)k'$, and $(a+bi'+cj'+dk')(w+xi'+yj'+zk') = (aw - bx - cy - dz) + (ax + bw + cz - dy)i' + (ay + cw + dx - bz)j' + (az + by + dw - cx)k'$

Quaternions are sometimes referred to as *hypercomplex* numbers, since they can be thought of as ordered pairs of complex numbers. The identification states if $q = a + bi' + cj' + dk'$ is a quaternion, we associate with q the ordered pair of complex numbers (z_1, z_2), where $z_1 = a + bi$ and $z_2 = c + di$. Written in this way, the addition of quaternions is accomplished "coordinate-wise":

$$(z_1, z_2) + (w_1, w_2) = (z_1 + w_1, z_2 + w_2),$$

while multiplication follows the rule:

$$(z_1, z_2)(w_1, w_2) = (z_1 w_1 - z_2 \overline{w}_2, \overline{z}_1 w_1 - w_2 \overline{z}_2),$$

where $\overline{z}$ represents the complex conjugate $a - bi$ of a complex number $z = a + bi$. While somewhat cumbersome, it is straightforward to verify that this addition and multiplication of ordered pairs of complex numbers mirrors the original definition of the quaternions.

The quaternions can be faithfully represented as 2x2 complex matrices by setting up the correspondence

$$M(a + bi' + cj' + dk') = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix},$$

or, if we consider the quaternions as ordered pairs of complex numbers, we have

$$M(z_1,z_2) = \begin{pmatrix} z_1 & z_2 \\ -\bar{z}_2 & \bar{z}_1 \end{pmatrix}.$$

Under this representation, we have $M(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $M(i') = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $M(j') = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $M(k') = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. We can verify that $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = M(-1)$, and the rest of the multiplication table for the matrix representatives of i', j', and k' is similarly verified to respect the multiplication table of i', j' and k'. In general, if $q_1 = a_1 + b_1i' + c_1j' + d_1k'$ and $q_2 = a_2 + b_2i' + c_2j' + d_2k'$ are two quaternions, then we have

$$M(q_1) + M(q_2) = \begin{pmatrix} a_1+b_1i & c_1+d_1i \\ -c_1+d_1i & a_1-b_1i \end{pmatrix} + \begin{pmatrix} a_2+b_2i & c_2+d_2i \\ -c_2+d_2i & a_2-b_2i \end{pmatrix}$$

$$= \begin{pmatrix} (a_1+a_2)+(b_1+b_2)i & (c_1+c_2)+(d_1+d_2)i \\ -(c_1+c_2)+(d_1+d_2)i & (a_1+a_2)-(b_1+b_2)i \end{pmatrix} = M(q_1 + q_2), \text{ and}$$

$$M(q_1)M(q_2) = \begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix}\begin{pmatrix} z_2 & w_2 \\ -\bar{w}_2 & \bar{z}_2 \end{pmatrix}$$

(where $z_1 = a_1 + b\,i$, $w = c_1 + d_1i$, $z_2 = a_2 + b_2i$, $w_2 = c_2 + d_2i$)

$$= \begin{pmatrix} z_1z_2-w_1\bar{w}_2 & z_1w_2+w_1\bar{z}_2 \\ -\bar{w}_1z_2-\bar{z}_1\bar{w}_2 & -\bar{w}_1w_2+\bar{z}_1\bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1z_2-w_1\bar{w}_2 & z_1w_2+w_1\bar{z}_2 \\ -(z_1w_2+w_1\bar{z}_2) & (z_1z_2-w_1\bar{w}_2 \end{pmatrix}$$

$= M(q_1q_2)$. The representation is certainly faithful, since $M(q_1) = M(q_2)$ if and only if $a_1 = a$, $b_1 = b_2$, $c_1 = c_2$, $d_1 = d_2$, i.e., $q_1 = q_2$.

Written in the form $q = a + bi' + cj' + dk'$, it seems quite a formidable task to determine under what conditions the quaternion q has a multiplicative inverse q^{-1}, whether or not there is a distinction between left and right inverses (owing to the noncommutativity of the multiplication), and exactly what form q^{-1} would take on when it does exist. Here the matrix representation comes in particularly handy. If we write $z = a + bi$ and $w = c + di$, then $M(q) = \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}$. This

matrix has an inverse if and only if the determinant $z\bar{z} + w\bar{w} = a^2 + b^2 + c^2 + d^2$ is nonzero. Thus, any nonzero quaternion has an inverse (which is "two-sided"), justifying the reference to skew field. Indeed, matrix theory also gives us the explicit form of this inverse, namely

$$M(q)^{-1} = \begin{pmatrix} \frac{\bar{z}}{z\bar{z} + w\bar{w}} & \frac{-w}{z\bar{z} + w\bar{w}} \\ \frac{\bar{w}}{z\bar{z} + w\bar{w}} & \frac{z}{z\bar{z} + w\bar{w}} \end{pmatrix},$$

so we have $q^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}\ (a - bi' - cj' - dk')$.

As an illustration of the quite bizarre nature of the quaternions, we consider the problem of determining the zeros of a polynomial with real coefficients. The main motivation for the construction of the complex numbers was the desire to determine zeros of all such polynomials, including $x^2 + 1$. If we denote the set of quaternions as Q, we might ask which quaternions satisfy the equation $x^2 + 1 = 0$. The reader may notice that we have at least three solutions, namely i', j', and k'. This is startling enough, as the degree of the polynomial is only 2. However, $x^2 + 1 = 0$ actually has ***infinitely*** many quaternionic roots! For example, if b is any real number such that $0 \le b \le 1$, and $c = \sqrt{1 - b^2}$, then $bi' + cj'$ is a zero of $x^2 + 1$, since $(bi' + cj')^2 = b^2i'^2 + bc(i'j' + j'i') + c^2j'^2 = b^2(-1) + bc(0) + c^2(-1) = -1$. (There are certainly many other zeros of $x^2 + 1$ which lie in Q besides these.)

Relationships among G, H, P, Z, R, C, and Q. In this closing section, we will tie all of the number systems considered in this article together via representation theory. We will show that all these number systems can be considered as subsystems of a ***single*** algebraic structure, namely the 2x2 complex matrices $M_2(C)$. For this to make any sense, all of our representations must be compatible. By this we mean that if two different systems "overlap," then their representations must match on the overlapping part. For example, we saw that our representations for G, H and P were compatible in this respect, since

each represented their common elements, the integers, in exactly the same way (as scalar matrices).

We have seen representations of G, H and P as integral 2x2 matrices, and we remind the reader that these are automatically also representations as complex 2x2 matrices. Similarly, the scalar representation of $\mathcal{R}$, namely

$$M(r) = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$$

for each $r \in \mathcal{R}$, can also be considered as a complex representation of the real numbers. Notice that this representation is compatible with those for G, H and P, since the integers (the subset of $\mathcal{R}$ which "overlaps" G, H, and P) are represented as scalar matrices still. How about the quaternions? Both $\mathcal{Z}$ and $\mathcal{R}$ can be considered as subsets of the quaternions by considering their elements to be particular quaternions with zero i', j', and k' parts. Fortunately, the representation we chose for Q is compatible with our representations of G, H, P, and $\mathcal{R}$, since a quaternion q = a (a either real or integer) has representative $M(q) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

The complex numbers C are another matter, since we have discussed two distinct faithful representations of the complex numbers as 2x2 complex matrices. The first of these we discussed was the real (hence automatically complex) representation which assigned to each complex number z = a + bi the matrix

$$M(z) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

The other representation discussed earlier was simply the scalar representation:

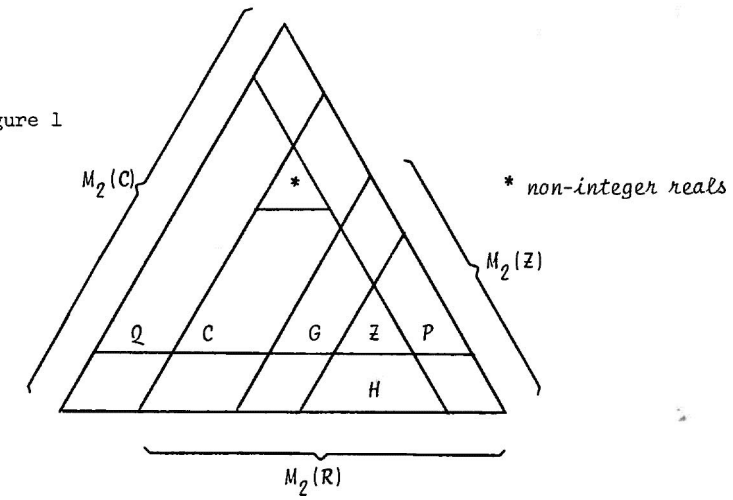
$$M(z) = \begin{pmatrix} z & 0 \\ 0 & z \end{pmatrix}$$

These are not the only representations of the complex numbers as 2x2 complex matrices. For example, $M(z) = \begin{pmatrix} a & bi \\ bi & a \end{pmatrix}$ defines a faithful representation of C distinct from either of the above ones. Which should we choose? Since the Gaussian integers are also complex numbers, our representation of the complex numbers should agree with that of G for all Gaussian integers. The scalar representation of

C is not compatible, unless we are willing to use the scalar representation $M(m + ni) = \begin{pmatrix} m+ni & 0 \\ 0 & m+ni \end{pmatrix}$ for the Gaussian integers also. Since we would lose some of the common ground among G, H, and P in this case, we choose instead to use the first representation $M(z) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, which agrees already with our representation of G, as well as with R.

Finally, we need to return to the quaternions to check that this chosen representation for C is also compatible with that for Q. There are several ways to consider C as a subset of Q, since i', j', and k' all behave like the imaginary square root of negative one. So the question remains which of the three, if any, we should identify as the complex number i in order to achieve compatibility of representations. We recall that the quaternions were represented as 2x2 complex matrices with $M(i') = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $M(j') = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $M(k') = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, so that j' is represented by the same matrix as i in our representation of the complex numbers. Hence, if we agree to consider complex numbers a + bi as being special quaternions of the form a + bj', all our representations are compatible in every respect. The beauty of the faithfulness of all these representations is that

Figure 1



we would be justified in actually defining G, H, P, $\mathbb{Z}$, R, C, and and Q as certain 2x2 complex matrices (though this is usually not done). If this is done, we arrive at the Venn diagram (Figure 1) showing the various inclusions.

Concluding Remarks. We have seen that matrices afford a useful way of representing many quite different kinds of number systems. To be accurate, in this article we have discussed the representation of rings. Representation theory can be used to describe many other types of algebraic structures. For instance, the representation of groups concerns representing each element of the group as an appropriate matrix with usual matrix multiplication paralleling the single group operation. As an example, $\mathbb{Z}_n$, the group of integers modulo n (with addition as the single operation), has a faithful representation as 2x2 real matrices via the identification:

$$M(k) = \begin{pmatrix} \cos\frac{k(2\pi)}{n} & \sin\frac{k(2\pi)}{n} \\ -\sin\frac{k(2\pi)}{n} & \cos\frac{k(2\pi)}{n} \end{pmatrix}; \quad k = 0,1,\ldots,(n-1).$$

We leave it to the reader to verify that $M(k)M(j) = M(k + j)$, where the addition is modulo n.

Commutative and noncommutative algebras, as well as Lie algebras (which have a non-associative multiplication defined) are other algebraic structures in which representation theory plays a major role in active research. It is safe to say that representation theory has earned an enduring reputation as a "unifying" tool in bringing together diverse topics in mathematics to the common ground of matrices.

READING LIST

1. Bold, B. and Wayne, A., *Number* Systems, ABC, New York, 1972.
2. Herstein, I. N., Topics in Algebra, 2nd edition, Xerox, Lexington, MA, 1975.
3. Humphreys, J. E., Introduction to Lie Algebras and Representation Theory, Graduate Texts in Mathematics, 9, Springer-Verlag, New York, 1972.
4. Lang, S., Algebra, Addison-Wesley, Reading, 1965.
5. Weyl, H., The Classical Groups, 2nd edition, Princeton University Press, 1946.

A THEOREM OF PHILIP HALL

by Barbara A. Benander
Cleveland State University

PART I: Introduction

The study of group theory is a relatively new area of mathematics. This challenging and exciting frontier has intrigued many mathematicians in recent years. As a result, these pioneers have bequeathed to the world of mathematics some very interesting findings. This paper will examine some of these findings, with an emphasis on the work of one individual.

Among the early group theorists was a mathematician named Ludwig Sylow (1832-1918). He was a noted speaker and many of his lectures were attended by enthusiasts in the field of group theory. For some, it was attendance at these talks which inspired them to produce results in this field.

Sylow himself was impressed by another mathematician, Augustin-Louis Cauchy. A theorem produced around 1835 by Cauchy caught the attention of Sylow. The theorem stated that every group whose order is divisible by a given prime p must contain at least one subgroup of order p. Nearly thirty years after Cauchy's finding, Sylow proudly presented his extension of it. Not surprisingly, this theorem was dubbed "Sylow's Theorem." It is stated in Part II of this paper.

Like Sylow, another mathematician was intrigued by Cauchy's theorem. His name was Philip Hall. Pursuing his interest in group theory, he went on to study Sylow's extension of Cauchy's theorem. The fruits of his labor can be found in a further extension of Cauchy's theorem. This new extension was first discovered by Hall in 1928. It is this theorem of Hall's which shall be proven in this paper. The validity of its converse shall also be demonstrated.

It is interesting to note that the diverse backgrounds of these men lend an international flavor to the study of groups. Cauchy was French, Sylow was from Norway and Hall hailed from England. And yet these individuals had very much in common. All were indefatigable

workers and men of uncommon scientific ability. More than that, they were united in their quest to learn more about group theory, an important and interesting branch of mathematics.

PART II: Theorems and Definitions Used in the Proofs of Philip Hall's Theorem and Its Converse

1. (Lagrange's Theorem). Let G be a group of finite order n and let H be a subgroup of G (written $H \leq G$), then the order of H divides the order of G.
2. (Sylow's Theorem). Every group whose order is divisible by $(p)^m$, but not by $(p)^{m+1}$, where p is a prime, contains a subgroup of order $(p)^m$, and all such subgroups are conjugate.
3. Let G be a group. If A and B are two finite subgroups of G, then
$$|AB| = \frac{|A||B|}{|A \cap B|}.$$
4. Let H be a normal subgroup of G (written $H \triangleleft G$), then G is solvable if and only if H and G/H are solvable.
5. Let N be a minimal normal subgroup of G (written $N \cdot \triangleleft G$). If N is solvable, then
   (i) N is abelian, and
   (ii) if N is finite, then N is an elementary abelian p-group.
6. Definition of "p-group":
   Let p be a prime. A group G is a p-group in case every element in G has order a power of p.
7. Definition of "solvable":
   Let G be a finite group. G is solvable if and only if there exists a series
   $$G = G > G_1 > \ldots > G = \{1\}$$
   such that G_i/G_{i+1} is cyclic of prime order, for $i = 0,1,\ldots, n-1$.
8. Definition of "minimal normal subgroup":
   A minimal normal subgroup N of G is a normal subgroup $\neq \{1\}$ that contains no proper subgroup that is normal in G.

PART III: A Proof of a Theorem of Philip Hall

Let G be a solvable group of order ab, where a and b are relatively prime. Then G contains at least one subgroup of order a, and any two such are conjugate.

Proof. The proof proceeds by induction on the order of G.

If G is solvable, then G contains a proper normal subgroup H. By Lagrange's Theorem, the order of H divides the order of G. Therefore, the order of H is a_1b_1, where a_1 divides a and b_1 divides b.

Case (i). $b_1 < b$.

If G is solvable and $H \triangleleft G$, then G/H is solvable (Th. 4, P.II). Thus G/H is a solvable group of order ab/a_1b_1 or $(a/a_1)(b/b_1)$. Since $|G/H| < |G|$, there is a subgroup A/H of G/H which has order a/a_1; that is, $|A/H| = a/a_1$.

Letting x represent the order of A, we then have $|A/H| = a/a_1 = x/a_1b_1$. From this it can be asserted that $x = ab_1 = |A|$. Since $ab_1 < ab$, $|A| < |G|$. Also, $A \leq G$ and any subgroup of a solvable group is solvable. Therefore, A is solvable. By induction, A contains a subgroup of order a, as desired.

Now suppose there are two subgroups of G, A and A , of order a. Let $k = |AH|$. $|A||H| = |A \cap H||AH|$ (Th. 3, P. II). This fact implies that $aa_1b_1 = |A \cap H| \cdot k$. We thus arrive at the fact that k divides aa_1b_1. Also, since $H \triangleleft G$, $AH \leq G$, which leads us to conclude that $|AH|$ divides $|G|$. Hence, k divides ab.

Let $k = k_ak_b$, where k_a and k_b are the prime factors of k which divide a and b, respectively. Then, if k divides aa_1b_1, k_b must divide b. And if k divides ab, then k_a divides a. Thus, k divides ab_1.

But, on the other hand, since $A \leq AH$ and $H \leq AH$, Lagrange's theorem requires that a divide k and that a_1b_1 divide k. Now the least common multiple of a and a_1b_1 is ab_1. And if two numbers divide the same number, their least common multiple also divides the number. Hence, ab_1 divides k.

Since k divides ab_1 and ab_1 divides k, it follows that $k = ab_1$.

A similar argument shows that $|A_1H| = ab_1$.

Thus, AH/H and A_1H/H are subgroups of G/H, both of order ab_1/a_1b_1, which equals a/a_1.

Again, using induction, AH/H is conjugate to A_1H/H in G/H. Thus, there exists an element x, in G, such that $(xH)^{-1}\,AH/H\,(xH) = A_1H/H$. And so we have $(x^{-1}H)\,AH/H\,(xH) = A_1H/H$. Let y be an element of AH. This implies that y = ah, with a in A and h in H. So for every y in AH, there exists an a_1 in A_1 such that the following is true: $(x^{-1}H)(yH)(xH) = a_1H$ or $x^{-1}yx(a_1)^{-1}H = H$. It follows that $x^{-1}yx(a_1)^{-1}$ is in H. This means that $x^{-1}yx(a_1)^{-1} = h$ for some h in H. Consequently, $x^{-1}yx = a_1H$. Hence, $x^{-1}yx$ is an element of A_1H.

Since $x^{-1}yx$ is in $x^{-1}(AH)x$, $x^{-1}H(AH)xH \subseteq AH$. But $|x^{-1}H(AH)xH| = |AH| = |A_1H|$, which implies that $x^{-1}H(AH)xH = A_1H$. Thus, AH and A_1H are conjugate in G. Therefore, xAx^{-1} and A are subgroups of A_1H of order a and so are conjugate by induction.

Case (ii). If G has a proper normal subgroup whose order is not divisible by b, then the theorem is proven. We therefore assume that b divides $|H|$, for every proper normal subgroup H. However, if H is a minimal normal subgroup, then $|H| = p^m$, where p is a prime (Th. 5, P.II). By Lagrange's theorem, p^m divides ab, which means that p^m divides a or p^m divides b. Also, b divides $|H|$ or b divides p^m. Consequently, p^m divides b.

We now have that b divides p^m and that p^m divides b. Therefore, $b = p^m$. Hence, H is a p-sylow subgroup of G. This fact, together with the fact that H is normal in G implies that H is the unique minimal normal subgroup of G.

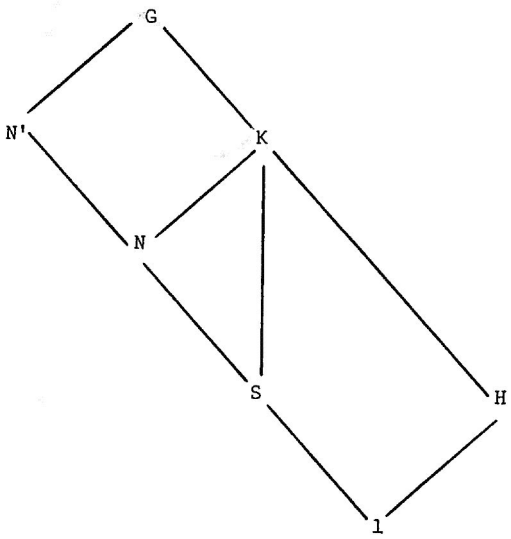
Now, because G is finite, every normal subgroup of G contains a minimal normal subgroup. Since H is the unique minimal normal subgroup, it is necessarily contained in every normal subgroup of G.

Let K/H be a minimal normal subgroup of G/H. The order of K/H is q^n, where q is a prime (Th. 5, P.II). Letting $x = |K|$, we have $|K/H| = x/(p)^m = q^n$. Hence, $x = p^m q^n = |K|$.

Let S be a q-sylow subgroup of K and N' be the normalizer of S in G. It shall be shown that $|N'| = a$. The diagram on the next page illustrates the situation.

Observe that $HS \leq K$. $|H||S| = |H \cap S||HS|$ (Th. 3, P.II). Since $|H \cap S| = 1$, $|H||S| = |HS|$. Hence, $|HS| = |K|$. Therefore, $K = HS$.

Now, $K \lhd G$ implies that $K^g = K$, for every g in G. $S \leq K$



means that $S^g \leq K^g = K$. Therefore, $S^g \leq K$. We may thus conclude that every conjugate of S in G lies in K.

Since $|S^g| = |S|$ for every g in G, S^g is a q-sylow subgroup of K. This means that S^g and S are conjugate in K. That is to say, there exists a k in K such that $(S^g)^k = S$. Hence, every conjugate of S in G is conjugate in K. Letting c represent the number of conjugates of S in G, the following equation results: $c = [G:N] = [K:N] = [HN:N] = [H:H \cap N]$. The third equality holds because $S \leq N$. That is to say, $N \geq S$ means that $HN \geq HS = K$. But $N, H \leq HS = K$ means that $NH \leq K$. Therefore, $HN = K$.

The last equality is demonstrated by appealing to Th. 3, P.II which states that $|HN| = (|H||N|)/|H \cap N|$. Dividing both sides of the equation by $|N|$ yields the following: $|HN|/|N| = |H|/|H \cap N|$. This last equation accounts for $[HN:N] = [H:H \cap N]$.

If we can show that $H \cap N = \{1\}$ our task will be facilitated quite considerably. For if $H \cap N = \{1\}$, then $c = |G|/|N'| = |H| = p^m$.

This leads to the conclusion that $(ab)/|N'| = p^m = b$ or $|N'| = a$.

This result shall be obtained in two stages. First, we will show that $H \cap N \subset Z(K)$, the center of K. Secondly, it will be demonstrated that $Z(K) = \{1\}$.

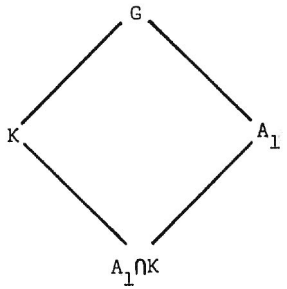
Let x be an element of $H \cap N$. If $k \in K$, then $k = hs$ with $h \in H$ and $s \in S$. Since $x \in H$ and H is abelian, x commutes with h. Now it remains to show that x commutes with s. Observe that $((x^{-1}s^{-1}x)s) \in S$ since $x \in N$ and $S \triangleleft N$. $(x^{-1}(s^{-1}xs)) \in H$ because H is normal. Hence, $(x^{-1}s^{-1}xs) \in S \cap H = \{1\}$, which implies that $xs = sx$. This allows us to claim that x commutes with s, as desired. Thus, $H \cap N \subset Z(K)$.

Finally, Z(K) is a characteristic subgroup of K, and $K \triangleleft G$ so Z(K) is normal in G. If $Z(K) \neq 1$, then Z(K) contains a minimal normal subgroup of G. Thus $H \leq Z(K)$, by the uniqueness of H.

Now, $H \leq Z(K)$ means that $hkh^{-1} = k$, for every k in K and for all h in H. Also, $K = HS$. That is, $k = hs$, for some $h \in H$ and some $s \in S$. Therefore, $S^k = S^{hs} = s^{-1}(h^{-1}Sh)s = s^{-1}Ss = S$. From this we arrive at the fact that $S \triangleleft K$ which tells us that S is characteristic in K and so $S \triangleleft G$. We now conclude that S contains H, the unique minimal normal subgroup of G. But this is a contradiction since $S = q^n$ and $H = p^n$. Thus our assumption that $Z(K) \neq 1$ has led us into a contradiction. Hence, $Z(K) = 1$.

Using the above results, namely that $H \cap N \subset Z(K)$ and $Z(K) = 1$, we may assert that $H \cap N = 1$ and $|N'| = a$.

Now suppose that A is another subgroup of G with order a. Observe that $|A_1K|$ is divisible by a and by $|K|$, which equals $p^m q^n$. We may conclude that $|A_1K| = |G|$ so that $A_1K = G$. We have the following diagram:



Since $A_1K = G$, $G/K = (A_1K)/K$. Hence, $G/K = (A_1K)/K \approx A_1/(A_1 \cap K)$. Observe that $|(A_1K)/K| = (ab)/(p^m q^n)$. Let $x = |A_1 \cap K|$. Then we have $|A_1/(A_1 \cap K)| = a/x$. So $(ab)/(p^m q^n) = a/x$ or $x = (ap^m q^n)/(ab) = q^n$.

Therefore, by the Sylow Theorem, $A_1 \cap K$ is conjugate to S in K. Also, for $r \in A_1$, note that $(A_1 \cap K)^r = (A_1)^r \cap K^r = A_1 \cap K$, since $K \triangleleft G$. Hence, $(A_1 \cap K) \triangleleft A_1$.

Having observed that $A_1 \cap K$ is conjugate to S in K, it follows that $A_1 \cap K = S^k$, for some $k \in K$. Thus $N_G(A_1 \cap K) = N_G(S)^k = (N')^k$. We thus conclude that $|N_G(A_1 \cap K)| = a$. Also, $A_1 \cap K \triangleleft A_1$ implies that $A_1 \leq N_G(A_1 \cap K)$. Hence, $A_1 = N_G(A_1 \cap K)$ and, as shown above, $N_G(A_1 \cap K)$ and N' are conjugate. This completes the proof of the theorem.

PART IV: A Proof of the Converse of Hall's Theorem

Let G be a finite group such that if $|G| = ab$, where a and b are relatively prime, then there exists a subgroup H of G and $|H| = a$, then G is solvable.

Proof. Let $|G| = (p_1)^{\delta 1}(p_2)^{\delta 2} \ldots (p_n)^{\delta n}$, where the p_i are prime and $p_i \neq p_j$ if $i \neq j$.

Case (i). $n = 1$

If $n = 1$, G is a p-group. It follows that G is nilpotent and solvable.

Case (ii). $n = 2$

If $n = 2$, G is a two prime group and is solvable by a theorem of Burnside. (W. Burnside, "On Groups of order $p^\alpha q^\beta$," Proceedings London Mathematical Society, Series 2, Vol. II (1904), pp. 432-437).

Case (iii). $n \geq 3$

Let T_i be the subgroup H for $b_i = (p_i)^{\delta i}$ and $a_i = |G|/b_i$, for $i = 1,2,\ldots,n$.

Then $|G/T_i| = (p_i)^{\delta i}$, so the indices of T_1, T_2, and T_3 are pairwise relatively prime.

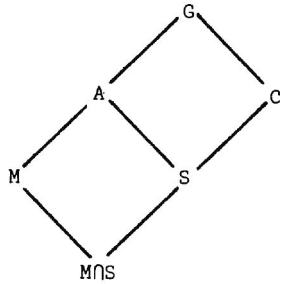
Since $|T_i \cap T_j| = |G|/((p_i)^{\delta i}(p_j)^{\delta j})$, each of the T_i will satisfy the hypothesis of the theorem. Hence, T_1, T_2 and T_3 are solvable by induction. The Three-Subgroup Theorem would serve very well at this point, for it would allow us to conclude that G is solvable. However, before drawing this desired conclusion, the Three-subgroup Theorem will be demonstrated.

The Three-Subgroup Theorem (Wielandt, 1960) states: Let A, B and C be subgroups of G, where $(|G/A|,|G/B|) = (|G/A|,|G/C|) = (|G/B|,|G/C|) = 1$. Also, A, Band C are solvable and $|G/A| = \mu$, $|G/B| = \delta$ and $|G/C| = \sigma$. Then G is solvable.

Proof. $G = AB = BC = AC$. Note that $1 \leq A \leq G$, $1 \leq B \leq G$ and $1 \leq C \leq G$.

Let $M \cdot \lhd A$ so that $|M| = p^n$. $(\delta,\sigma) = 1$ so that p does not divide δ or p does not divide σ. Without loss of generality, we shall say that p does not divide σ.

Let $S = A \cap C$. The following diagram should aid in the understanding of the situation:



Since p does not divide σ which equals $|G/C|$, p does not divide $|A/S|$. Observe that $S \leq MS \leq A$. Also, from Th. 3, P.II, $|MS| = (|M||S|)/|M \cap S| = |M/(M \cap S)| \cdot |S|$. If p divides $|M/(M \cap S)|$ then p divides $|A/S|$. But this is a contradiction. Hence, p does not divide $|M/(M \cap S)|$, so that $|M/(M \cap S)| = 1$. Therefore, $M = M \cap S$ which implies that $M \leq S$. From this we can say that $M \leq C$.

Let $g \varepsilon G$. Then $g = ac$, with $a \varepsilon A$ and $c \varepsilon C$. $M^g = M^{ac} = M^c \leq C$. Thus $M^G \leq C$ which implies that M^G is solvable.

Let π: $G \to G/(M^G)$ be the natural homomorphism. Then $\pi(A)$, $\pi(B)$ and $\pi(C)$ are solvable. Also, $|\pi(G)/\pi(A)| = |\pi(G)/\pi(B)| = |\pi(G)/\pi(C)| = 1$. These last two facts imply that $G/(M^G)$ is solvable.

We now have that M^G and $G/(M^G)$ are solvable. Therefore G is solvable (Th. 4, P.II).

Having proved the Three-Subgroup Theorem, we will now apply it to complete the proof of the converse of Hall's theorem.

Recall that T_1, T_2 and T_3 are subgroups of G and are solvable. We have shown that their indices are pairwise relatively prime. From the Three-Subgroup Theorem, G is solvable. Thus the validity of the converse of Hall's theorem is demonstrated.

REFERENCES

1. Burnside, William, "On Groups of Order $p^a q^\beta$," *The Journal of London Mathematical Society*, 1904, II, 432-437.

2. Cajori, Florian, *A History of Mathematics*, New York: Macmillan Co., 1929.

3. Hall, Philip, "A Note on Solvable Groups," *The Journal of London Mathematical Society*, 1928, III, 98-105.

4. Horwath, Darrell J., *Helmut W. Wielandt: Topics in the Theory of Composite Groups*, Lecture Notes, University of Wisconsin, 1967.

5. Rotman, Joseph, *The Theory of Groups: An Introduction*, Boston: Allyn and Bacon, Inc., 1966.

6. Sylow, Ludwig, *Math. Ann.*, 1872, 588.

About the author -

As an undergraduate, Dr. Benander was an active member of the Ohio Lambda chapter of Pi Mu Epsilon at John Carroll University where she majored in mathematics. She earned a Ph. P. in Mathematics at Kent State University. Currently, Barbara is an assistant professor in the computer science department at Cleveland State University.

About the paper -

This paper was written in 1972 when the author was an undergraduate.. The paper was awarded First Prize in the essay contest sponsored by the Ohio Lambda Chapter of Pi Mu Epsilon.

Editor's Note.

The Pi Mu Epsilon Journal was founded in 1949 and is dedicated to undergraduate and beginning graduate students interested in mathematics. Submitted articles, announcements and contributions to the Puzzle Section and Problem Department of the Journal should be directed toward this group.

Undergraduate and beginning graduate students are strongly urged to submit papm to the Journal for consideration and possible publication. Student papm will be given top priority.

Expository articles by professionals in all areas of mathematics are especially welcome.

THE ROLE OF RUSSELL'S PARADOX IN THE DEVELOPMENT OF TWENTIETH CENTURY MATHEMATICS

by Karen P. Middleton
Keene State. College

In mathematics, as in most other disciplines, practitioners have attempted to define the foundation or basis upon which their discipline is ostensibly constructed. Not only were the classical Greeks the first mathematicians to ponder the basis of math, but also, the culmination of the Greek mathematical enterprise, Euclid's ***Elements,*** stood as the foundation of math for more than 2000 years. Euclid used the principles of Aristotle's deductive logic to derive hundreds of geometric theorems from only a few basic assumptions, or axioms. Since Aristotle's logical method was accepted as infallible, thinkers could not reject the reults of Euclid's theorems, although they have occasionally challenged his axioms. Davis and Hersh (1981, p. 325) refer to the "Euclid myth ... that the books of Euclid contain truths about the universe which are clear and indubitable."

Until the late nineteenth century, both philosophers and mathematicians regarded geometry as "the firmest, most reliable branch of knowledge" (Davis & Hersh, 330). At that time, a number of mathematicians decided to try to reformulate arithmetic according to the laws of deductive reasoning, just as Euclid had done for geometry. Many arithmetic results had been used for centuries without being proven, because they seemed to be a matter of common sense. The German mathematician Gottlob Frege worked for ten years to derive theorems of arithmetic from just a few assumptions. He wanted to replace intuitive notions of the real number system with a precise axiomatic system, to render arithmetic more "rigorous" (Wilder, 1973, p. 175). He was nearly finished with his two-volume work *Grundgesetze der Arithmetik (Fundamental Laws of Arithmetic)* in 1902, and he believed that it was "no less a model of certitude than the ***Elements***" (Guillen, 1983, p. 15).

Unfortunately, the British philosopher-mathematician Bertrand Russell had noticed a paradox, a flaw in logic, in Frege's final manuscript. Frege himself agreed that the flaw was serious enough to ruin his entire effort:

"A scientist can hardly meet with anything more undesirable than to have the foundation give way just as the work is finished. In this position I was put by a letter from Mr. Bertrand Russell as the work was nearly through the press" (Guillen, p. 15).

The contradiction that Russell discovered lies in set theory-;.- which Georg Cantor had developed during the later nineteenth century. Set theory had quickly become indispensable to mathematics; it was used to define number and to discuss infinity. The notion of a set had seemed quite simple and straight-forward; it was believed that any sensible verbal description could be used to denote a set. Russell took this basic idea and, for the first time, really tested it mentally. He realized that while most sets are not members of themselves (the set of teaspoons is not another teaspoon), there are a few sets which are members of themselves: for example, the set of all ideas is itself an idea. The set of all sets that have more than five members itself has more than five members; therefore this set is also a member of itself.

Suppose we take M as the set of all sets which are members of themselves, and N as the set of all sets which are not members of themselves. N itself is a set, so it must belong to either M or N If N belongs to N, then it is a member of itself, so it must belong to *M.* But M and N are mutually exclusive sets, so if *N* belongs to *M,* it cannot belong to *N* (Kline, 1972, p. 1184).

Russell's paradox is described by W. V. Quine (1962, p. 90) as follows: "What of the class of all classes that are not members of themselves? Since its members are the nonself-members, it qualifies as a member of itself if and only if it is not. It is and it is not."

Russell's paradox caused a serious crisis in the foundations of mathematics precisely because it could not be resolved through logic. There was no apparent logical fallacy in Russell's thinking. Quine (p. 85) terms this type of paradox an "antinomy," and contrasts antinomy with paradoxes which contain logical fallacies. Famous examples of the latter include the English mathematician Augustus De Morgan's proof that $2 = 1$:

'Let $x = 1$. Then $x^2 = x$. . So $x^2 - 1 = x - 1$. Dividing both sides by $x - 1$, we conclude that $x + 1 = 1$; that is, since $x = 1$, $2 = 1$" (Quine, p. 84). The logical fallacy here is in the division

by $x - 1$ which is 0.

An interesting and ancient verbal paradox concerns the village where there lives a barber who shaves all and only those men in the village who do not shave themselves. So -- does the barber shave himself? It would seem he shaves himself if and only if he doesn't. Quine (p. 84) concludes that we rid ourselves of this paradox by the realization that no village can contain such a barber; we reduce this paradox to absurdity.

Some of the most famous paradoxes in mathematical history were proposed by the Greek philosopher Zeno of Elea. Four of his paradoxes concern motion, inlcuding the race between Achilles and the Tortoise. Zeno concluded that if the Tortoise has a head start, Achilles can never catch up, because whenever he arrives at the point where the Tortoise was, the Tortoise will have moved ahead a little. Today we can see the fallacy in this paradox: the Greeks must have thought that an infinite succession of intervals would add up to an infinite interval (Quine, p. 89). When mathematicians came to understand convergent series, Zeno's paradox was solved.

Rather than containing a fallacy, however, Russell's antinomy demonstrated that a "trusted pattern of thinking was found wanting" (Quine, p. 90). The trusted pattern of reasoning was the basic idea behind set theory, that for any condition you can think of there must be a set whose members meet that condition. Actually, as we have seen in Russell's antinomy, there can be no class that has as members the classes that are not members of themselves.

Quine points out, interestingly enough, that to the ancient Greeks Zeno's paradoxes probably qualified as genuine antinomies. Since the Greeks did not know about convergent series, they could not have detected the logical fallacies in Zeno's arguments. To them, it might have seemed that Zeno had introduced a crisis situation into mathematics, just as Russell did more than 2000 years later. Davis and Hersh (p. 226) propose that Euclid's axiomatic treatment of such "intuitive" geometric objects as "line" and "point" might have been in response to Zeno's paradox, to forestall the problems Zeno had raised. In the same way, we now think the Greeks concentrated on geometry "to avoid the difficulties posed by the discovery of incommensurable magnitudes" (Wilder, p. 176).

In response to Russell's antinomy, three distinct schools of mathematical thinking have attempted to resolve the problem. None has succeeded in obtaining universal agreement among mathematicians.

Bertrand Russell and the English mathematician Alfred North Whitehead led the Logicists, who sought a way to reformulate set theory whichwouldavoid or nullify the Russell paradox. They contended that mathematics is a branch of logic, and that all of math can be reduced to logic. They hoped to restore "certainty" to mathematics through logic. Russell and Whitehead published *Principia Mathematica* between 1910 and 1913; in this enormous work, mathematics was deduced from logic using complex symbolic language. The authors proposed that the terms "set" and "ordered pair," and the laws governing sets and ordered pairs, belong to the discipline of logic rather than math. They then showed that "the laws of arithmetic and the rest of the mathematics of number are related to those of logic in the same way as the theorems of geometry are related to its axioms" (Barker, 1964, p. 80).

Russell and Whitehead dealt with Russell's paradox through their theory of types. According to this theory, all the entities of set theory, such as sets, sets of sets, sets of sets of sets, etc., are arranged in a hierarchy of levels, or types, and each entity can belong to just one type. No set can have members of types other than the next lower type. They specified that "whatever involves all members of a collection must not itself be a member of the collection" (Kline, p. 1195). By thus restricting the logical axioms relating to sets, Russell and Whitehead were able to retain the basic idea behind set theory, that for every statable condition there exists a set containing all and only those things which satisfy the condition. As Barker (p. 91) summarizes, Russell and Whitehead avoided the paradox "by narrowing the range of sentences in set theory that are to count as making sense."

More recently, most mathematicians have disagreed with the Russell-Whitehead thesis that math and logic are identical. Rather, mathematical logic has been extensively developed as a separate branch of mathematics. In 1962 Leon Henkin wrote that the basic concepts of math can be expressed in logical terms, but as J. Fang asked in a review of Henkin's paper (Fang, 1964, p. 47), are

mathematics and physics identical "because the basic concepts of all physics can be expressed in terms of mathematics?"

Russell and Whitehead were hoping that logic would give certainty back to mathematics. However, as Jagit Singh (1959, p. 274) points out, logic is "certain" because it doesn't deal with substance. Logic is concerned with the nature and rules of reasoning; we use logic to deduce valid conclusions from given premises. "Logic studies the relations between propositions independently of what each proposition is about." Singh finds it surprising that logistic , mathematicians like Russell and Whitehead could so readily disregard the substance of math.

A very different approach to mathematics was taken by the Intuitionist school. It was founded in the late 1800's by Leopold Kronecker, who stated that Cantor's work on transfinite numbers and set theory was mysticism rather than mathematics. Kronecker accepted little in mathematics beyond the whole numbers, which he said are given to us by a fundamental intuition. He rejected irrational numbers, for example, as non-existent. Kronecker stood alone in his philosophy until the controversy over Russell's paradox had begun. Beginning in 1908, the Dutch topologist L. E. J. Brouwer took up Kronecker's positon and elaborated it. He demonstrated that the concept of natural whole numbers came from the perception of the passage of time, a fundamental human intuition. Brouwer maintained that "all mathematics should be based constructively on the natural numbers" (Davis and Hersh, p. 334). No mathematical object exists unless it can be given by a construction, in a finite number of steps, starting with the natural numbers.

Brouwer and the Intuitionists rejected the use of proof by contradiction. A good example is Brouwer's treatment of Fermat's last theorem, in which Fermat asserted without proof that there are no natural numbers for n greater than 2 which satisfy the equation $x^n + y^n = z^n$. Mathematicians have tried but failed to prove or disprove this theorem; Intuitionists feel that since it can be neither proved nor disproved, then it may be neither true nor false. It may be a "meaningful statement possessing neither truth nor falsity" (Barker, p. 76).

Brouwer asserts that mathematical ideas are in the human

mind "prior to language, logic, and experience" (Kline, p. 1200). He does not recognize the necessity of deducing mathematical conclusions from axioms. Therefore, to the Intuitionists, Russell's paradox is unimportant. The Intuitionists find logic to be a function of language, not of mathematics. Furthermore, they claim that paradoxes such as Russell's result from "the unjustified extension of the laws of logic from the finite to the infinite" (Wilder, p. 177).

A third major school of mathematical philosophy arose early in the twentieth century. The Formalists were led by David Hilbert, whose first paper in the field appeared in 1904; at that time, he attempted to establish a basis for the number system without using the theory of sets, and he argued against Kronecker's contention that the irrationals don't exist. Hilbert's major papers appeared during the 1920's, when he sought to defend mathematics from the Intuitionist viewpoint; he feared that they were trying "to save math by throwing overboard all that which is troublesome...they would chop up and mangle the science" (Davis and Hersh, p. 335).

Hilbert introduced a formal language and rules of inference so that every proof of a classical theorem could be mechanically checked. He also introduced rules for transforming formulas, referred to as meta-mathematics. Hilbert was attempting to place mathematics on a certain and reliable foundation by eliminating meaning from the mathematical symbols. He wrote that the symbols themselves are the essence of math, and that they no longer stand for any idealized physical objects (Kline, p. 1204).

Since Hilbert and the Formalists purged their mathematical language of semantic content, they found that the mathematical failure revealed by Russell's paradox actually lay in language, not in math. For example, the origin of many paradoxes, including Russell's, lies in the ambiguity of the word "all." If we state "All rules have exceptions," we have a paradox if we define "all" to include this statement (Guillen, p. 17). This paradox and many others are thus semantic, rather than logical, and can be avoided by carefully removing any meaning from logic. Hilbert and his followers have often been criticized for trying to make mathematics "safe by turning it into a meaningless game" (Davis and Hersh, p. 336). Nonetheless, Hilbert's philosophy, somewhat changed, has evolved

into the predominant attitude in modern mathematics: today, Formalists define math as the science of rigorous proof.

Each of the three major schools of mathematical philosophy attempted to re-establish the mathematical certainty that seemed to have been lost with Russell's paradox. None succeeded, but mathematicians had hope until, in 1931, the German logician Kurt Gödel's incompleteness theorems showed that certainty could not be obtained by any method founded on traditional logic. Thus the Formalist and Logicist schools were doomed to failure. The Intuitionist school failed because it condemns so much of classical math.

Mathematicians today tend to treat this philosophical upheaval of the early twentieth century as if it never happened. If they do not quite believe that their discipline rests on a foundation of certainty, they certainly do their day-to-day work as if it doesn't really matter. The predominant belief among non-mathematicians is that mathematics is an exact science resting on a base of certainty. The late philosopher Imre Lakatos in ***Proofs and Refutations*** (1976) showed that math is really like the natural sciences, that it is fallible, that "it too grows by the criticism and correction of theories which are never entirely free of ambiguity or the possibility of error or oversight" (Davis and Hersch, p. 347). Lakatos emphasized informal math, math in the process of growth and discovery, which is actually math as most mathematicians know it. The great value of Russell's paradox has been its contribution to the growth of mathematics; the fact that we cannot yet really resolve it is of much less importance than the search.

REFERENCES

1. Barker, Stephen F., ***Philosophy of Mathematics,*** Englewood Cliffs, NJ: Prentice-Hall, 1964.
2. Davis, Philip J., and Reuben Hersh, ***The Mathematical Experience,*** Boston: Houghton Mifflin, 1981.
3. Fang, J., Review of Leon Henkin's "Are Logic and Mathematics Identical?", ***Philosophica*** *Mathematica,* 1964, *1,* 45-50.
4. Fang, J., "What Is, and Ought to Be, Philosophy of Mathematics?", ***Philosophica*** *Mathematica,* 1967, ***4,*** 71-75.

5. Guillen, Michael, ***Bridges to Infinity: the Human Side of Mathematics,*** Los Angeles: Jeremy P. Tarcher, Inc., 1983.
6. Henkin, Leon, "Are Logic and Mathematics Identical?", ***Science,*** 1962, 138, 788-794.
7. Kline, Morris, ***Mathematical Thought from Ancient to*** *Modern Times,* New York: Oxford University Press, 1972.
8. Quine, W. V., "Paradox", ***Scientific American,*** 1962, ***206,*** 84-96.
9. Singh, Jagjit, ***Great Ideas of Modern Mathematics: their Nature and Use,*** New York: Dover Pubs., 1959.
10. Wilder, Raymond L., "Relativity of Standards of Mathematical Rigor." ***Dictionary of the History of Ideas,*** Philip P. Wiener, ed., New York: Charles Scribner's Sons, 1973.

About the. ***author*** -

Karen is a mathematics student at Keene ***State College*** *and expects to* ***complete course work in December 1986.***

About the. ***paper*** - *Karen* ***wrote this paper for*** *a come. in the.* ***history of mathematics taught*** *by* ***Dr. Joseph Witkowski.***

✲

Matching Prize Fund.

If your Chapter presents awards for Outstanding Mathematical Papers or for Student Achievement in Mathematics, you may apply to the National Office for an amount equal to that spent by your Chapter up to a maximum of fifty dollars.

Posters

A supply of 10" by 14" Fraternity Crests me. available. One. in each color combination will be sent free to tach Chapter upon request. Additional posters ate available at the following rates

(1) *Purple on Goldenrod Stock* $1.50/dozen
(2) *Purple on Lavender on Goldenrod* $2.00/dozen

Send requests and orders to ***Dr. Richard*** *A. Good.* ***Secretary-Treasurer,*** *Department of Mathematics, University of Maryland, College Park, MD 20742.*

THE ACTUARIAL PROFESSION: ONE OF THE BEST KEPT SECRETS OF THE BUSINESS WORLD

by Nancie L. Merritt
Insurance Services Office, Inc.

For some college undergraduates, becoming an actuary conjures up images of sitting in some isolated corner, crunching out numbers that only other mathematicians can understand. Other students aren't even aware that the actuarial profession exists as a career alternative until almost ready to graduate. If you have a strong background in math, and would like to be part of a highly interesting, demanding and rewarding field, then an actuarial career might be for you.

The Profession. Just what is an actuary? Skilled mathematicians, actuaries are business professionals that have the ability to analyze and solve complex problems in a number of disciplines. According to the Casualty Actuarial Society, actuaries "help design plans to reduce the financial impact of the expected and unexpected things that happen to people, like illnesses, accidents, unemployment, or premature death. They evaluate the financial risk a company takes when it sells an insurance policy or offers a pension program." (The Casualty Actuarial Society promotes and increases the knowledge of actuarial science, and maintains high qualification standards for the profession.)

While most actuaries work within the insurance industry, others are employed by the government, health industry, actuarial consulting firms, accounting firms, and private corporations. Using advanced math formulas and data often compiled from millions of cases, actuaries can determine risks, establish probabilities, and help insurance companies set premiums. Whenever a person buys homeowners or automobile insurance, for instance, actuaries have already determined the probability of an insurable event occurring, its average cost, and the appropriate premium to be charged.

In many insurance companies, no specific college training is needed to become an actuary. But candidates need a ***strong*** background in math or statistics. Math, physics, economics, computer science, or

engineering majors usually have the necessary quantitative background to succeed as actuaries.

Actuaries are involved in much more than number crunching; they need to use both their "analytical" and "people" skills in this line of work. Most companies hiring actuaries look for people who not only possess good math skills, but demonstrate clear communication skills as well.

As business professionals, actuaries need to have a broad understanding of the business world and the general environment. So students preparing for the career need to incorporate English, business writing, and speech classes into their curriculum. It is also helpful to round out their studies with courses in business, philosophy, and logic.

In addition, many companies sponsor actuarial intern programs during the summer break. Participating in an internship is an ideal way to get a feel for what the actuarial profession entails. Students should seriously consider applying for a summer program during the breaks between their junior and senior years.

The Actuarial Exams. To obtain professional qualification to practice as an actuary, candidates usually need to become Fellows in the Society of Actuaries (for life and health insurance and pension planning), or the Casualty Actuarial Society (for property and casualty insurance). Actuarial recruits are expected to pass ten comprehensive examinations given by either the CAS or SOA.

Offered twice a year, the exams cover several interrelated fields crucial to an actuary's career development: mathematics, statistics, economics, risk theory, accounting, law, and forecasting. Taking all ten exams can take anywhere from four to ten years - or longer - to complete. But students can begin careers as actuaries once they receive their undergraduate degree. They can work to develop their actuarial skills as they pass the exams. When a recruit has completed the first seven exams, he or she becomes an associate of the CAS or SOA. Those who pass all ten exams earn their Fellowship.

While no formal training is necessary, most insurance companies want students to have taken at least one actuarial exam while in college. For some actuarial candidates, the additional

pressure of the exams proves burdensome. Completing the exams requires self discipline and the ability to study without supervision - qualities that can be nurtured while still in school.

For those actuarial candidates who are willing and able, the opportunity to move into a company's upper ranks is there. Depending on your own ability and experience - and if you are regularly passing actuarial exams - you will be rewarded with a regular series of exam raises and additional career opportunities.

An Actuarial Career at ISO. Insurance Services Office, Inc., or ISO, specializes in actuarial services. ISO is one of the largest employers of actuaries in the property/casualty insurance industry. It is not, however, an insurance company. Rather, ISO assists insurance companies by collecting, analyzing, and producing accurate and timely data, which its clients - over 1300 property and casualty insurers - use to make important business decisions.

Essentially, ISO is a consulting organization. The company employs actuarial techniques to develop projected industry costs for various kinds, or lines, of insurance. Every year, ISO uses data from 800 million insurance records to develop advisory rate information. Based on these records and its actuarial expertise, ISO provides advice to clients for 16 different lines of insurance.

Many ISO actuaries conduct research to predict future economic and social trends that can have an impact on the property/casualty insurance industry. They also deal with insurance underwriters, lawyers, and regulators on a regular basis, and are involved in testifying before state regulatory hearings.

Ken Levine, actuarial assistant, sr. in ISO's Commercial Casualty Division, is a recent ISO inductee, and is glad to have joined the ranks of actuarialprofessionals. Ken graduated with a math degree from Rensselaer Polytechnic Institute. "When I heard about the actuarial profession from my high school guidance counselor, I didn't give it much thought. At RPI, I took a number of business courses to complement my math studies and enjoyed them very much.

"By my senior year, I felt that becoming an actuary in the insurance industry would provide me with the perfect opportunity to apply my math skills in a business environment. What attracted me to ISO was its role as the provider of information to the property/casualty insurance industry."

There's no denying that this is a challenging job. If you are looking for a meal ticket that doesn't involve heavy lifting, then the actuarial profession is probably not for you. But if you're interested in breaking new ground, making worthwhile contributions to a company, and applying your math skills in a business environment, then you're going to fit right in.

For more information about the actuarial profession, contact the Casualty Actuarial Society at One Penn Plaza, 250 West 34th Street, New York, New York 10119. And for more information about ISO, write to ISO's College Recruitment Coordinator at 160 Water Street, New York, New York 10038.

The Actuarial Examinations

Associate Examinations:

Part 1. General Mathematics
Part 2. Probability and Statistics
Part 3. (A) Applied Statistical Analysis, (B) Operations Research and (C) Numerical Analysis
Part 4. (A) Mathematics of Compound Interest, (B) Life and Casualty Contingencies and (C) Credibility Theory
Part 5. (A) Principles of Economics, (B) Theory of Risk and Insurance, (C) Policy Forms and Coverages and (D) Underwriting and Marketing
Part 6. (A) Principles of Ratemaking and (B) Data for Ratemaking
Part 7. (A) Insurance Accounting, (B) Expense Analysis and Published Financial Information and (C) Premium, Loss and Expense Reserves

Fellowship Examinations:

Part 8. (A) Insurance Law, Supervision and Regulation, (B) Statutory Insurance and (C) NAIC (the proceedings of the National Association of Insurance Commissioners)
Part 9. (A) Advanced Ratemaking and (B) Individual Risk Rating
Part 10. (A) Financial Operations of Insurance Companies, (B) Reinsurance and Excess Rating, (C) Forecasting and (D) Current Events and Issues

THE FOCAL DISTANCE OF A CONIC SECTION

by Ali R. Amir-Moéz
Texas Tech University

In his book, ***Mathematical Recreations*** and ***Essays*** [1], Walter W. Rouse Ball, under the title of Ninth Fallacy, mentions that every ellipse is a circle. This is very interesting and pertains to the problem of extrema on the boundary. In this note we study the focal distance for conic sections and its extrema.

1. The Ellipse. Consider the ellipse

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \quad a > b > 0.$$

Let the foci be F(-c,0) and G(c,0), as in Figure 1. Let P be a point on the ellipse.

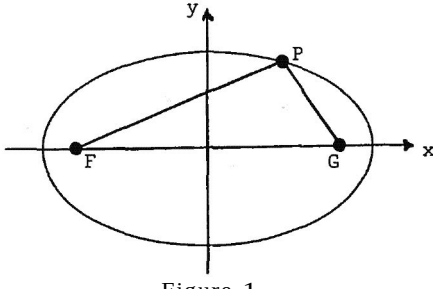


Figure 1

We shall calculate PF = r, which we call the focal distance for P.

From the distance formula,

$$r^2 = (x + c)^2 + y^2.$$

On the other hand, from the equation of the ellipse,

$$y^2 = \frac{b^2}{a^2}(a^2 - x^2) = \frac{a^2 - c^2}{a^2}(a^2 - x^2) = (1 - e^2)(a^2 - x^2),$$

where e = c/a is the eccentricity of the ellipse. Thus

$$r^2 = x^2 + 2cx + c^2 + (1 - e^2)(a^2 - x^2)$$

$$= e^2x^2 + 2cx + a^2$$

$$= e^2x^2 + 2eax + a^2$$

$$= (ex + a)^2.$$

Hence, $r = a + ex$.

The domain of the function $r = r(x)$ is

$$D = \{x: |x| \leq a\}.$$

This implies that

$$a - c \leq a + ex \leq a + c.$$

Consequently,

$$r = a + ex > 0,$$

and a + c and a - c are the maximum and the minimum of r, respectively, and are achieved at the boundary of the domain of r. That is, the extema occur when P is a vertex of the ellipse.

In [1], it is stated: "Since dr/dx = e is constant, r has no maximum and minimum, and it (the ellipse) must be a circle." Indeed, Professor Ball was teasing.

One can easily calculate PG and obtain

$$PG = \ell = a - ex.$$

Again, from $|x| \leq a$, one can show that

$$a - c \leq a - ex \leq a + c.$$

2. The Hyperbola. Consider the hyperbola

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1.$$

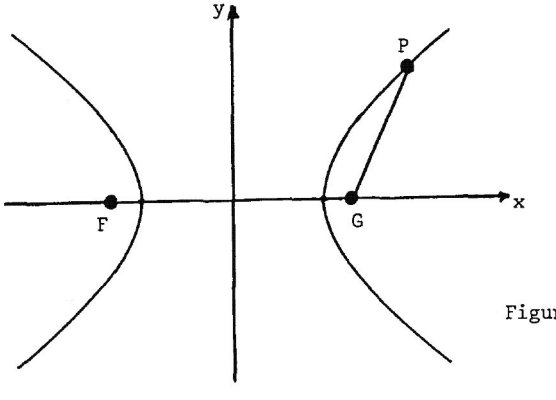


Figure 2

As in Figure 2, let the foci be G(c,0) and F(-c,0). We calculate PG = r, where

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

In this case,

$$y^2 = \frac{b^2}{a^2}(x^2 - a^2) = \frac{c^2 - a^2}{a^2}(x^2 - a^2) = (e^2 - 1)(x^2 - a^2).$$

Thus

$$r^2 = x^2 - 2cx + c^2 + (e^2 - 1)(x^2 - a^2)$$

$$= e^2x^2 - 2cx + a^2$$

$$= e^2x^2 - 2eax + a^2$$

$$= (ex - a)^2,$$

where, once again, we have used c = ea.

Hence, $r = |ex - a|$. The domain of the function r = r(x) is

$$D = \{x: |x| \geq a\}.$$

Considering $x \geq a$, we get $ex - a \geq c - a$. In this case, $r = ex - a$. For $x \leq -a$, we obtain $ex - a \leq -c - a$ and we must choose $r = a - ex$.

In all cases, the minimum of r is attained at the boundary of the domain; that is, when P is a vertex of the hyperbola.

The reader may study the focal distance PF which is quite similar to the one of PG.

3. The Parabola. Consider the parabola

$$y^2 = 4ax, \quad a > 0$$

with the focus F(a,0), as in Figure 3. It is clear that

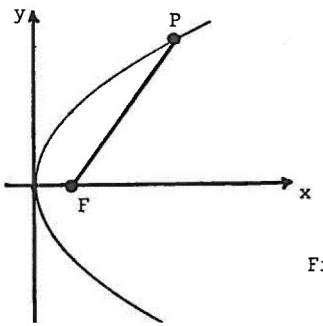


Figure 3

$$PF = r = x + a.$$

Again, we obtain the minimum value of r on the boundary of the domain of r; that is, when P is the vertex of the parabola.

4. Problems. If we choose a point on an axis of any of the conics mentioned above, the corresponding radial distances may or may not have all the extrema on the boundary. These problems may be of some interest to students. We shall give samples.

(i). Consider the ellipse in Figure 4. Let A(p,0) be a point on the major axis of the ellipse and let P be on the ellipse. Obtain the maximum and the minimum of AP.

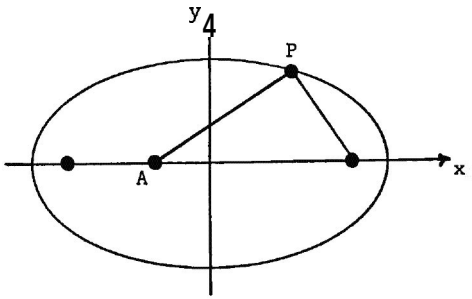


Figure 4

The maximum occurs on the boundary, but it is interesting to obtain a necessary and sufficient condition so that the minimum does not occur on the boundary. The reader may show that the condition is $|p| < c^2/a$. The case of $|p| = c^2/a$ is interesting to study.

(ii). For the parabola and hyperbola similar problems may be posed. Of course, there is no maximum. One need only discuss the problem of the occurrence of the minimum on the boundary.

REFERENCE

1. Ball, Walter W. Rouse, *Mathematical Recreations and Essays*, Toronto: University of Toronto Press, 1974.

THREE FAMILIAR RESULTS VIA THE MEAN VALUE THEOREM

by Norman Schaumberger
Bronx Community College

In this note we use one application of the mean value theorem to obtain three significant results.

The first is the familiar double inequality for e that states that for all positive integers n

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

Secondly,

$$(2) \qquad \frac{(n+1)^n}{n} < n! < \frac{(n+1)^{n+1}}{n}.$$

Although (2) is not as good as Stirling's formula it can carry the student a long way in approximating n!.

The third is

$$(3) \qquad \lim_{n\to\infty} \frac{(n!)^{1/n}}{n} = \frac{1}{e}$$

which is usually not proved until the student is exposed to Stirling's formula. (See, for example, ***Advanced Calculus*** by Taylor, Ginn 6 Co., 1955, p. 688.)

Using the mean value theorem with $f(x) = x\log x - x$, we have

$$\frac{[(k+1)\log(k+1) - (k+1)] - [k\log k - k]}{(k+1) - k} = \log c$$

where $k \geq 1$ and $c \in (k, k+1)$.

Hence

$$(4) \quad \log k < (k+1)\log(k+1) - k\log k - 1 < \log(k+1).$$

To get (1) we rewrite (4) as

$$k\log(k+1) - k\log k < 1 < (k+1)\log(k+1) - (k+1)\log k$$

or

$$\log\left(\frac{k+1}{k}\right)^k < 1 < \log\left(\frac{k+1}{k}\right)^{k+1}.$$

It follows that

$$\left(1 + \frac{1}{k}\right)^k < e < \left(1 + \frac{1}{k}\right)^{k+1}.$$

To obtain (2), we put k = n, n - 1, n - 2, ..., 1 in (4) and add. Thus

$$\sum_{1}^{n} \log k < (n+1)\log(n+1) - 1\cdot\log(1) - n < \sum_{2}^{n+1} \log k.$$

Consequently

$$\log n! < \log(n+1)^{n+1} - \log e^n < \log(n+1)!$$

or

$$\log \frac{(n+1)^n}{n^n} < \log n! < \log \frac{(n+1)^{n+1}}{e^n}.$$

Hence

$$\frac{(n+1)^n}{e^n} < n! < \frac{(n+1)^{n+1}}{e^n}.$$

Result (3) now follows by writing the above as

$$\frac{n+1}{e} < (n!)^{1/n} < \frac{(n+1)^{(n+1)/n}}{e}$$

or

$$\frac{n+1}{n}\cdot\frac{1}{e} < \frac{(n!)^{1/n}}{n} < \frac{n+1}{n}\cdot(n+1)^{1/n}\cdot\frac{1}{e}.$$

As $n \to \infty$, $\frac{n+1}{n} \to 1$ and $(n+1)^{1/n} \to 1$, so that

$$\lim_{n\to\infty} \frac{(n!)^{1/n}}{n} = \frac{1}{e}.$$

✲

ANOTHER APPROACH TO $e^\pi > \pi^e$

by Norman Schaumberger
Bronx Community College

Using the mean value theorem for integrals, we have

$$\int_e^\pi \frac{dx}{x} = \frac{1}{c}(\pi - e), \quad e < c < \pi.$$

Hence, $\ln(\pi) - \ln(e) < \frac{(\pi - e)}{e} = \frac{\pi}{e} - \ln(e)$.

Thus, $e\ln(\pi) < \pi\ln(e)$, or $\pi^e < e^\pi$.

MARCEL RIESZ - AN ANECDOTE

by J. L. Brenner
10 Phillips Road
Palo Alto, CA 94303

Marcel Riesz was a great mathematician in more ways than one. He believed in good food and drink, and went 300 pounds. Thus he stood out in a crowd. Especially was he known to all who attended a conference in College Park, Maryland, in 1954, since he was the after-dinner speaker at the banquet.

The banquet must have continued into the late hours, since when I appeared the next morning (late myself) Riesz was not yet seated. Like me, he took a seat in the back of the room. I hardly need remark that I was not as well-known to Riesz as he was to me. I couldn't have mistaken him.

Riesz immediately began fidgeting, searching first in one pocket and then in another. He continued this so persistently that soon I myself was looking into all my pockets. It didn't help him for me to do this, but eventually he found what he was looking for -- his eyeglasses. He put them on, leaned far forward to read my name tag, and then extended his hand smiling. "Riesz is my name," he chortled. He was already acquainted with everybody else, and wished to score one hundred percent.

Editor's Note

Marcel Riesz (1886-1969) was a prizewinner in the Eötvös Mathematical Competition in Hungary in 1904.

Spend one oh two semesters of your junior/senior years in Hungary, a country with a tong tradition of excellence in mathematics research and education. Take part in BUDAPEST SEMESTERS IN MATHEMATICS.

An Incredible Experience!

David Wagner, Participant

For information and application forms write to Prof. W. T. Trotter, Jh., Department of Mathematics, University of South Carolina, Columbia, S. C. 29208.

CALL FOR NOMINATIONS

Elections for national officers of the Pi Mu Epsilon Fraternity will be held in the Spring of 1987. The three-year terms of office will begin July 1, 1987.

The Nominating Committee consists of Richard V. Andree, University of Oklahoma, Chairman, J. Sutherland Frame, Michigan State University, and E. Maurice Beesley, University of Nevada. The committee will meet at the 1986 Pi Mu Epsilon National Conference at the University of California at Berkeley, August 3 - August 6.

The committee solicits recommendations for nominees from the membership. Please submit names and addresses of possible nominees to Milton D. Cox, President, Pi Mu Epsilon, Department of Mathematics and Statistics, Miami University, Oxford, Ohio 45056, or to any member of the Nominating Committee, before July 1, 1986.

Additional nominations for officers may be made in accordance with Sections 2. and 3. of Article V. of the Constitution and By-Laws which are reproduced below.

ARTICLE V. NATIONAL ORGANIZATION

Section 2. Officers. The Officers of the fraternity shall be President, Vice-president, Secretary-Treasurer, **Editor,** and four Councillors. These eight, together with the most recent past President shall constitute the Council of the fraternity, and shall serve without compensation.

Section 3. Election of Officers. The Officers shall be elected by the chapters to serve for a term of three years beginning July 1 every third year. They shall, however, hold office until their successors are elected and qualified. Nominations shall be made by a nominating committee appointed by the President. This committee shall nominate at least three candidates suitable for the office of President, at least one each for the offices of Secretary-Treasurer, Editor, and at least six for the four offices of Councillor. Additional nominations may be made by the Council, a General Convention, or any chapter of the fraternity prior to the month in which ballots are mailed to the chapters. The names of all nominees shall be submitted on a ballot to the chapters by the Secretary before January 31 preceding the beginning of the new term. Ballots shall indicate a first and second choice for President, one choice each for Secretary-Treasurer and for Editor, and four choices for Councillor. Decisions shall be based on a plurality of chapter votes cast for each office. The Vice-president shall be selected from the remaining candidates for the office of President by tallying each ballot for the preferred remaining candidate, **i.e.,** first choice candidate, unless the first choice candidate was elected President, in which case the second choice candidate shall receive the vote. In case of a tie among two or more candidates for an office, the out-going Council shall choose from such candidates.

Vacancies in the Council shall be filled for the balance of the term by a majority vote of the remaining Council upon nomination of the President.

1986 NATIONAL PI MU EPSILON MEETING

The Annual Pi Mu Epsilon National Meeting will be at the University of California at Berkeley from Sunday, August 3, through Wednesday, August 6, concurrently with the International Congress of Mathematicians (ICM–86). Pi Mu Epsilon meetings will be held in the evenings to avoid conflict with the ICM meetings during the day.

Student paper presenters and student delegates (non–presenters) are needed. Talks are to be fifteen minutes in length and may include any area of mathematics or its application. Talks may be on either the expository level or on the research level; both are encouraged. Mathematical topics in computing are also welcome.

Each chapter is eligible to apply for air travel support up to a (chapter) total of six hundred dollars ($600) for students presenting papers or up to a (chapter) total of three hundred dollars ($300) for delegates (non–presenters).

Ordinary registration for ICM–86 is $125. Students have the option of earning free registration by working ten (10) hours for ICM–86. Contact your chapter advisor for detailed information, registration forms and the "Information and Helpful Hints" sheet.

✲

REGIONAL MEETINGS

Many regional meetings of the Mathematical Association of America regularly have sessions for the presentation of student papers. If two or more colleges and at least one local chapter of Pi Mu Epsilon help sponsor, on participate in, iuch sessions, financial help up to $50 is available.. Write to Dr. Richard A. Good, Secretary-Treasurer, Department of Mathematics, University of Maryland, College Park, MD 20742.

✲

AWARDS CERTIFICATES

YoWL chapter can make use of the Pi Mu Epsilon Award Certficates available to help you recognize mathematical achievements of your students. Write to Richard A. Good, Secretray-Treasurer, Department of Mathematics, University of Maryland, College Park, MD 20742.

THE THIRTEENTH ANNUAL PI MU EPSILON STUDENT CONFERENCE

AT

MIAMI UNIVERSITY

IN

OXFORD, OHIO

OCTOBER 3-4, 1986

WE INVITE YOU TO JOIN US! THERE WILL BE SESSIONS OF THE STUDENT CONFERENCE ON FRIDAY EVENING AND SATURDAY AFTERNOON. FREE OVERNIGHT LODGING FOR ALL STUDENTS WILL BE ARRANGED WITH MIAMI STUDENTS. EACH STUDENT SHOULD BRING A SLEEPING BAG. ALL STUDENT GUESTS ARE INVITED TO A FREE FRIDAY EVENING PIZZA PARTY SUPPER AND SPEAKERS WILL BE TREATED TO A SATURDAY NOON PICNIC LUNCH. TALKS MAY BE ON ANY TOPIC RELATED TO MATHEMATICS, STATISTICS OR COMPUTING. WE WELCOME ITEMS RANGING FROM EXPOSITORY TO RESEARCH, INTERESTING APPLICATIONS, PROBLEMS, SUMMER EMPLOYMENT, ETC. PRESENTATION TIME SHOULD BE FIFTEEN OR THIRTY MINUTES.

WE NEED YOUR TITLE, PRESENTATION TIME (15 OR 30 MINUTES), PREFERRED DATE (FRIDAY OR SATURDAY) AND A 50 (APPROXIMATELY) WORD ABSTRACT BY SEPTEMBER 25, 1986.

PLEASE SEND TO

PROFESSOR MILTON D. COX
DEPARTMENT OF MATHEMATICS AND STATISTICS
MIAMI UNIVERSITY
OXFORD, OHIO 45056

WE ALSO ENCOURAGE YOU TO ATTEND THE CONFERENCE ON "DISCRETE MATHEMATICS" WHICH BEGINS FRIDAY AFTERNOON, OCTOBER 3. FEATURED SPEAKERS INCLUDE RON GRAHAM AND ALAN TUCKER. CONTACT US FOR MORE DETAILS.

H E L P ! H E L P ! H E L P !

ST. NORBERT COLLEGE

Presents

Our First Regional Pi Mu Epsilon Meeting

in

De Pere, Wisconsin (Green Bay)

November 7–8, 1986

We need your help at the inaugural event! Our goal is to have speakers for Friday evening and Saturday morning- In order to do so, we need YOUR creativity, no reasonable talk will be refused! (We do hope, however, that this talk will be related to mathematics, computer science or to work experiences, applications, etc.)

Your title, time of presentation (15 or 30 minutes) and a 30–70 word abstract are required by 10 October 1986.

Please send to:

Professor Rick Poss
Department of Mathematics
St. Norbert College
De Pere, Wisconsin 54115

Phone: 414–337–3198

There will be no registration fee. "All students will be provided with free housing (bring a sleeping bag). There will be a free party on Friday evening. Please contact us for further details.

H E L P ! **H E L P !** H E L P !

ARML Seeks Host Colleges for Its Annual Competitions

The American Regions Mathematics League is seeking colleges, preferably east of the Mississippi River, to host **ARML** competitions in 1988 and beyond. The annual competition. takes place in late May or early June. Accommodations are needed for one to three nights for approximately 800 students. Facilities are also needed for breakfast and lunch on the Saturday of the conference.

Colleges willing to host such a conference for the nations's top high school mathematics students should **write** J. Bryan Sullivan, 17 **Woodside** Dr., Sterling, MA 01564.

✲

CRYPTOLOGIA ANNUAL

UNDERGRADUATE PAPER COMPETITION

IN CRYPTOLOGY

WE ANNOUNCE THIS CONTEST TO ENCOURAGE THE STUDY OF ALL ASPECTS OF CRYPTOLOGY IN THE UNDERGRADUATE CURRICULA.

FIRST PRIZE: THREE HUNDRED DOLLARS

CLOSING DATE: 1 JANUARY

TOPIC MAY BE IN AMY AREA OF CRYPTOLOGY
TECHNICAL, HISTORICAL, AND LITERARY SUBJECTS

PAPERS MUST BE NO MORE THAN TWENTY TYPEWRITTEN PAGES IN LENGTH, DOUBLE SPACED **AND** FULLY REFERENCED. FOUR COPIES MUST BE SUBMITTED. AUTHORS SHOULD KEEP ONE COPY. PAPERS ARE TO BE ORIGINAL WORKS WHICH HAVE NOT BEEN PUBLISHED PREVIOUSLY.

THE PAPERS WILL BE JUDGED BY THE CRYPTOLOGIA EDITORS AND THE WINNER WILL BE ANNOUNCED ON 1 APRIL WITH PUBLICATION OF THE WINNING PAPER IN THE JULY ISSUE OF CRYPTOLOGIA.

THE COMPETITION IS UNDERWRITTEN BY A GENEROUS GIFT FROM BOSHRA **H.** MAKAR, PROFESSOR OF MATHEMATICS, SAINT PETER'S COLLEGE, JERSEY CITY, NEW JERSEY.

INQUIRIES, SUBMISSIONS AND SUBSCRIPTION INFORMATION:

CRYPTOLOGIA, EDITORIAL OFFICE
ROSE **HULMAN** INSTITUTE OF TECHNOLOGY
TERRE HAUTE, INDIANA 47803

PUZZLE SECTION

Edited by

Joseph D. E. Konhauser

The PUZZLE SECTION is for the enjoyment of those readers who ewe addicted to working doublecrostics or who find an occasional mathematical puzzle attractive. We consider mathematical puzzles to be problems whose solutions consist of answers immediately recognizable as correct by simple observation and requiring little formal proof. Material submitted and not used here will be sent to the Problem Editor if deemed appropriate for the PROBLEM DEPARTMENT.

Address all, proposed puzzles and puzzle solutions to Professor Joseph D. E. Konhauser, Mathematics and Computer Science Department, Macalester College, St. Paul, Minnesota 55105. Deadlines for puzzles appearing in the Fall Issue will be the next February 15, and for pussies appearing in the Spring Issue will be the next September 15.

Mathacrostic No. 22

Proposed by Joseph V. E. Konhauser

Macalester College, St. Paul, Minnesota

The word puzzle on pages **260** and **261** is a keyed anagram. The **241** letters to be entered in the diagram in the numbered spaces will be identical with those in the **25** keyed words at the matching numbers. The key numbers have been entered in the diagram to assist in constructing the solution. When completed, the initial letters of the words will give the name of an author and the title of a book; the completed diagram will be a quotation from that book. For an example, see the solution to the last mathacrostic on page **259**.

GRAFFITO

" ... one of,the things that sets puzzleheads off from the. saner members of society is that we do enjoy making things tougher for OWLselves."

Thomas H. Middleton

SOLUTION

Mathacrostic No. 21. (See Fall 1985 Issue) (proposed by Joseph D. E. Konhauser, Macalester Cortege, St. Paul, Minnesota).

Words:

A. Miter
B. Lightweight
C. Phonatory Bands
D. Rorschach
E. Ultima
F. Equiaffinity
G. Invest
H. The absolute
I. Tu-whit-tu-whoo
J. Aborigine
K. Rawindsonde
L. Ternary rings
M. Ablepsia
N. Nychthemeron
O. Dense-in-itself
P. Tower of Babel
Q. Hubble's constant
R. Effulgent
S. Chrestomathy
T. Ouchless
U. Miscellany
V. Passion to know
W. Ungulae
X. Touchstone
Y. Eyepoint
Z. Rabatment

First Letters: M. L. PRUEITT ART AND THE COMPUTER

Quotation: Behind each image abides an untold story. ... Only the programmers can fully see the beauty of, their work, the labyrinthine pathways woven among the. subunits of, instructions, the subtle twists in Logic., the elaborate sequence of, operations, and the synergism with which all components function to bring about a final result.

Solved by: **Jeanette Bickley**, Webster Groves High School, MO; **Victor G. FESER**, Mary College, Bismarck, ND; **Robert Forsberg**, Lexington, MA; **Robert C. Gebhardt**, Hopatcong, NJ; **Dr. Theodor Kaufman**, Winthrop-University Hospital, Mineola, NY; **Beth and Ron Prielipp**, Bethany College, Lindsborg, KS, and **Robert Prielipp**, University of Wisconsin-Oshkosh.

Errata

In listing the. names of the. solvers of, Mathacrostic # 20, that of, Barbara Zeeberg, Denver, Colorado, was incorrectly spelled.

In Mathacrostic # 20, word K. was incorrectly spelled. There is no d between the. n and the. s in any acceptable spelling of, the. wold "Rawinsonde."

Please accept my apologies.

Mathacrostic # 22

1 G	2 E	3 M		4 T	5 A	6 R	7 F	8 V	9 Q		10 M	11 G	12 O
13 W	14 T	15 E	16 X		17 R	18 L	19 H	20 W	21 A	22 S	23 M	24 G	25 T
26 V		27 N	28 R	29 X	30 P	31 G		32 C	33 V		34 J	35 X	36 F
37 H	38 U	39 C	40 I		41 M	42 H		43 C	44 A		45 K	46 R	47 X
48 W		49 K	50 U		51 H	52 S		53 U	54 G	55 P	56 E	57 I	58 R
59 X	60 B	61 N		62 I	63 C	64 U		65 D	66 Y		67 G	68 O	
69 J	70 T	71 B	72 L	73 N	74 V	75 Q		76 G	77 I	78 M		79 O	80 D
81 Q	82 W	83 A	84 U	85 E	86 I	87 C	88 B		89 J	90 H	91 B		92 P
93 X	94 G	95 C	96 E	97 S	98 K	99 O	100 L	101 W		102 A	103 F		104 K
105 G	106 Y		107 I	108 K		109 O	110 Q	111 T	112 L	113 H	114 J	115 R	116 V
117 E	118 A	119 B	120 P		121 K	122 N	123 B		124 R	125 K	126 P	127 D	
128 O	129 N		130 H	131 C		132 U	133 T	134 E	135 V	136 F	137 M	138 A	
139 S	140 Q		141 I	142 H	143 O		144 L	145 M	146 W	147 V	148 R	149 X	
150 T	151 N	152 Y		153 W	154 U		155 L	156 E	157 B		158 J	159 B	160 N
	161 G	162 Y	163 L	164 F	165 R	166 E	167 V	168 W	169 Q		170 N	171 K	172 B
	173 W	174 E	175 L	176 G	177 T	178 Y	179 X		180 D	181 N		182 D	183 U
184 B	185 S	186 N	187 J	188 K	189 W	190 G		191 K	192 R	193 I	194 M	195 V	196 H
197 U	198 G	199 Q		200 R	201 W	202 B		203 M	204 G	205 E	206 W		207 Q
208 N		209 J	210 W		211 R	212 V	213 X	214 L	215 I	216 A		217 H	218 N
	219 D	220 C	221 K		222 M	223 G	224 E	225 X	226 I	227 L	228 P	229 K	230 Y
	231 B	232 U		233 G	234 S	235 X		236 T	237 S	238 A	239 W	240 Q	241 X

Definitions

A. conjecture

B. his Newtonian prediction was verified in 1758 (full name)

C. adjunct edifice

D. said of a convex body whose every hyperplane of support has at most one point of contact with the body

E. theories which have revolutionized our ideas about the early universe (2 wds.)

F. enlarging gradually

G. Forrest Mims' word for digital watches, portable stereos, electronic calculators, transistor radios, pocket televisions, and home computers

H. taking up of fluid by a colloidal system resulting in swelling

I. very restricted methods of proof, as proposed by Hilbert

J. in Christianity, its rays are likened to the Holy Spirit's seven gifts

K. establish convincingly as accurate, true, real or genuine

L. manikin-shaped

M. the purest luster (2 wds.)

N. for each positive integer n > 2, they are vertices of a regular n-gon (3 wds.)

O. rotate faster than

P. lessen

Q. frequency

R. tally used in France by bakers in rural areas when they sold bread on credit (2 wds.)

S. a popfly, for example (2 wds.)

T. in mathematics, the Halmos-introduced symbol ∎ used to indicate the end of a proof

U. imperfectly circular (comp.)

V. a molecular species which contains separate centers of positive and negative charge; e.g., methyl orange

W. Maupertuis' 1736 expedition to Lapland to measure the length of an arc of one degree on one of the earth's meridians earned him this title (2 wds.)

X. for graphs F_1 and F_2, the least positive integer p such that for every graph G of order p either G contains F_1 as a subgraph or $\bar{G}$ contains F_2 as a subgraph (2 wds.)

Y. any special delicacy

Words

118 83 138 44 238 102 5 21 216

157 91 184 231 202 123 159 71 119 60 172 88

95 43 87 220 63 39 32 131

80 180 219 65 182 127

224 96 134 156 166 2 117 205 56 174 15 85

7 36 136 164 103

31 54 190 24 161 1 198 67 11 204 94 176

76 233 223 105

113 19 130 37 217 196 142 51 42 90

62 141 226 107 193 86 40 77 57 215

69 89 187 114 209 34 158

121 104 229 171 221 191 108 49 188 98 45 125

112 155 144 18 163 100 214 72 227 175

203 222 137 78 41 10 194 23 145 3

186 129 160 170 27 208 181 151 122 73 61 218

68 109 128 143 79 12 99

30 92 126 228 55 120

81 140 207 240 9 110 75 169 199

17 192 148 58 46 28 6 211 124 165 200 115

185 22 52 237 139 234 97

14 177 4 150 236 111 25 133 70

38 183 50 154 232 64 197 132 84 53

74 135 147 195 212 167 8 116 33 26

20 189 168 13 173 82 206 201 239 48 101 153

210 146

235 47 93 149 29 179 16 59 241 35 225 213

162 230 66 152 106 178

COMMENTS ON PUZZLES 1 - 6, FALL 1985

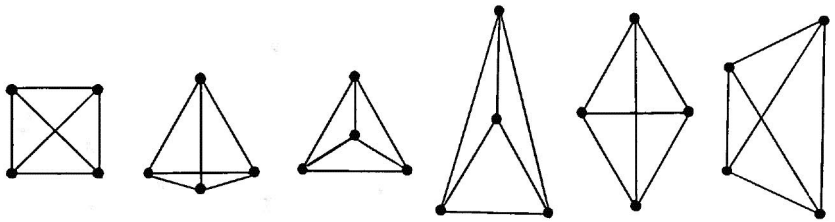
Brian Conrad wrote that *Puzzle # 1*, with k = 4, appears on page 48 of ***Games For The Superintelligent*** by James Fixx, Doubleday & Co., Inc., 1972. **Robert Prielipp** sent a reference to Problem 24 on page 12 of ***The USSR Olympiad Problem Book*** by D. 0. Shklarsky, N. N. Chentzov and I. M. Yaglom [(revised and edited by Irving Sussman and translated by John Maykovich), W. H. Freeman and Company, San Francisco and London, 19621. A proof that a solution exists only for k = 4 Is given on pages 114-117. Other correct responses to *Puzzle # 1* were received from **Mark Evans, John H. Scott** and **Victor G. Feser.** For Puzzle # 2, **Brian Conrad** and **Victor G. Feser** submitted

$$(-1 + 23) \div (\sqrt{4} + 5) = 22/7.$$

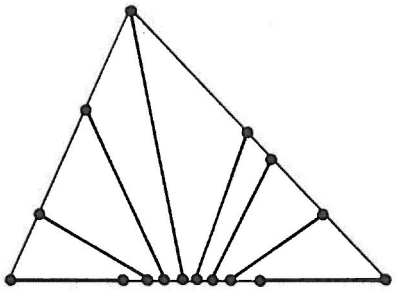
John H. Scott, who asked us to be broadminded about the conditions, submitted

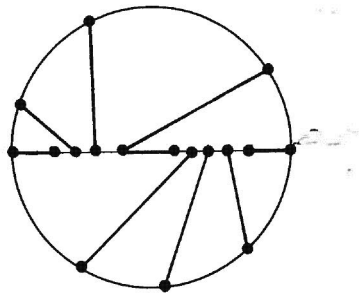
$$\frac{1 \times 2 \quad + \quad 4 \times 5}{3 + 4} = \frac{22}{7}.$$

For Part a. of *Puzzle # 3*, there are six ways of arranging four points in the plane so that the six distances between pairs of points fall into just two classes. These are shown below. Only partial responses were



were received for Part b. of *Puzzle # 3.* The correct answer to Part b. is 27. Only one of these arrangements - the vertices of a regular pentagon - is a planar arrangement. For a complete description of the other 26 arrangements, see the paper ***On Euclidean Sets Having Only Two Distances Between Points. I and II.*** by S. J. Einhorn and I. J. Schoenberg, *KONINKL. NEDERL.* AKADEMIE *VAN WETEN SCHAPPEN - AMSIERDAM, Proceedings, Series A, 69, No. 4* and *Indag. Math., 28, No. 4, 1966.* Only two responses were submitted for Puzzle # 4. That of **Leroy F. Meyers** was an analytical description of the graphics which follow.





Responses to Puzzle # 5 were received from **James E. Campbell, Victor G. Feser, Mark Evans, John M. Howell** and **John H. Scott. Victor G. Feser** put it this way " **...** the vertices of a regular pentagon with edges adjusted just right **... .**" A pentagon with edge length about 0.6498 will do it. For Puzzle # 6 **Victor G. Feser, Robert Prielipp, John M. Howell John H. Scott** and **James E. Campbell** submitted essentially equivalent solutions - all triples of the form $(4y, y, -2y)$, $y \neq 0$.

List of Responders: **James E. Campbell** *(3,5,6)*, **Brian Conrad** *(1,2)*, **Mark Evans** *(1,3,5)*, **Victor G. Feser** *(1,2,3,4,5,6)*, **John M. Howell** *(3,5,6)*, **Leroy F. Meyers** *(4)*, **Robert Prielipp** *(1,6)* and **John H. Scott** *(1,2,3,5,6)*.

PUZZLES FOR SOLUTION

1. *Proposed* by *Brian Conrad, Coram, New* Yohk.

Using the usual arithmetic symbols and the digits 5, 4, 3, 2, 1 in that order from left to right, are you able to form 22/7? If not, how close can you come to 22/7? What is the closest value to 22/7 that you can obtain by using the usual arithmetic symbols and the digits 1, 2, 3, 4 and 5 in that order both from left to right and from right to left? For example,

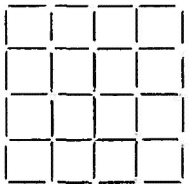
$$-12 \div (3 + 4) + 5 = 23/7 = (5 + 4^3) \div 21.$$

2. *Proposed* by *Robert Forsberg, Lexington, Massachusetts.*

Find a six-digit number such that starting at the left successive groups of four form three consecutive four-digit numbers.

3. *From the booklet Four by Four by Ernest Ranucci.*

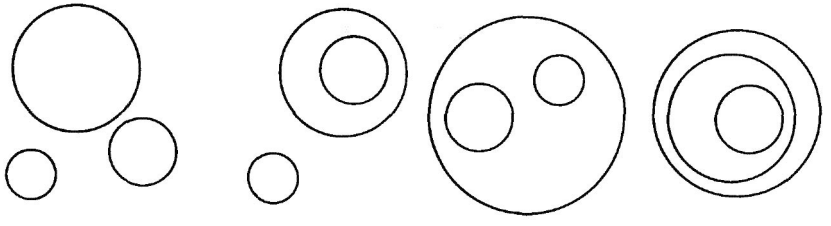
Imagine the "grid" below to be made of 40 matchsticks.



What is the smallest number of matchsticks which must be removed so that in the configuration that remains thematchsticksare not parts of the sides of a square of any size? The answer given is ten. Are you able to lower it to nine?

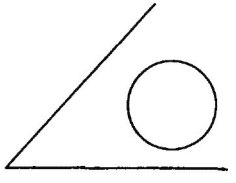
4. *Proposed by Joe Konhauser, Macalester College, St. Paul, Minnesota.*

In the plane, as shown below, three circles can be arranged in four ways so as to have no points of intersection. In three-space, in how many different ways can five spheres be so arranged?



5. *Proposed by Joe Konhauser, Macalester College, St. Paul, Minnesota.*

Given a circle interior to an angle, as shown, for which point on the circle is the sum of the distances from the sides of the angle least?



PROBLEM DEPARTMENT

Edited by Clayton W. Dodge
University of Maine

This department welcomes problems believed to be new and at a level appropriate for the readers of this journal. Old problems displaying novel and elegant methods, of solution are also invited. Proposals should be accompanied by solutions if available and by any information that will assist the editor. An asterisk (*) preceding a problem number indicates that the proposer did not submit a solution.

All communications should be addressed to C. W. Dodge, Math. Dept., University of Maine, Orono, ME 04469. Please submit each proposal and solution preferably typed on clearly written on a separate sheet [one side only) properly identified with name and address. Solutions to problems in this issue should be mailed by December 15, 1986.

Problems for Solution

613. *Proposed by Martha Matticks, Veazie, Maine.*

Use a bit of number theory to solve this alphametric that pays homage to geometry, algebra and analysis. Find that solution in base 7 yielding a prime *ANAL*.

$$\begin{array}{r} GEOM \\ +\ ALG \\ \hline ANAL \end{array}$$

614. *Proposed by Leon Bankoff, Los Angeles, California, and the editor.*

A 10,000-meter section of straight railroad track expands 1 meter and buckles into a circular arc. How high above ground is the middle of the arc? [This is an old problem and easy to solve using ordinary trigonometry. It is repeated here because the answer is of unexpected magnitude.]

615. *Proposed by William S. Cariens, Lorain County Community College, Elyria, Ohio.*

Although several years retired, the eminent numerologist

Professor Euclide Pasquale Bombasto Umbugio still solves problems with the same prowess and efficiency he always has had. His native country, Guayazuala, still cannot afford a computer, but they do have a pocket four-function calculator to which he has access. He is trying to find the sum of the abscissas of the seven points of intersection of the seventh-degree polynomial

$$f(x) = x^7 - 3x^6 - 13x^5 + 55x^4 - 36x^3 - 52x^2 + 48x$$

with its derivative polynomial. He has laboriously found one intersection at x = 1.3177227. Help the kindly, old professor to find his sum without resorting to a computer.

616. *Proposed by Dmitry P. Mavlo, Moscow, USSR.*

Prove that in any triangle

$$\frac{\tan\frac{A}{2} + \tan\frac{B}{2} + \tan\frac{C}{2}}{\cot\frac{A}{2} + \cot\frac{B}{2} + \cot\frac{C}{2}} \leq \frac{8}{27} + \left(\tan\frac{A}{2}\tan\frac{B}{2}\tan\frac{C}{2}\right)^2$$

with equality if and only if the triangle is equilateral.

617. *Proposed by Titus Canby, Adjustable Wrench Company, Buffalo, NY Yolk.*

It is known (The Two-Year College *Mathematics* Journal, problem 226, September 1982, page 277) that a 7 x 7 x 7 box can be packed with a maximum of forty 1 x 2 x 4 bricks, requiring 23 cubic units of unoccupied space. How many such bricks can be packed into a 5 x 5 x 5 cubic box?

618. *Proposed by John M. Howell, Littlerock, California.*

(i) Find when the sum of the squares of four consecutive integers is divisible by 3.

(ii) Repeat part (i) for the sum of the squares of four consecutive odd or four consecutive even integers.

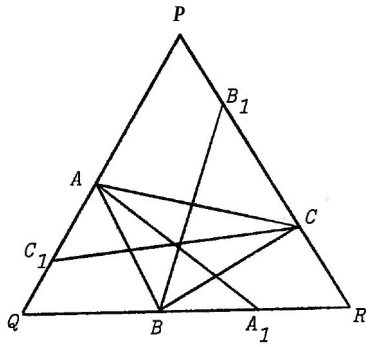
619. *Proposed by Victor G. Feser, Mary College, Bismarck, North Dakota..*

Find the largest value of x such that $x = \sin x = \tan x$, correct to 3, 4, 5, 6, 7, and 8 decimal places.

***620.** *Proposed by Jack Garfunkel, Flushing, NY York.*

A triangle ABC is inscribed in an equilateral triangle PQR.

The angle bisectors of triangle ABC are drawn and extended to meet the sides of triangle PQR in points A_1, B_1, C_1. Now draw the angle bisectors of triangle $A_1B_1C_1$ to meet the sides of triangle PQR at A_2, B_2, C_2. Repeat the procedure. Prove or disprove that triangle $A_nB_nC_n$ tends to equilateral as n tends to infinity. (This result has been proved when a circle is used instead of triangle PQR.)



621. *Proposed by R. S. Luthar, University of Wisconsin Center at Janesville.*

(i) Characterize all triangles whose angles and whose sides are both in arithmetic progression.

(ii) Characterize all triangles whose angles are in arithmetic progression and whose sides are in geometric progression.

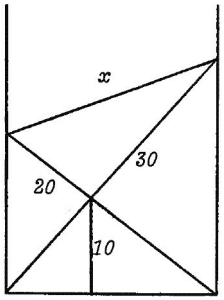
622. *Proposed by Walter Blumberg, Coral Springs, Florida.*

Let point P be the center of an equilateral triangle ABC and let c be any circle centered at P and lying entirely within the triangle Let BR and CS be tangents to the circle such that point R is closer to C than to A and S is closer to A than to B. Prove that line RS bisects side BC.

623. *Proposed by John M. Howell, Littlerock, California.*

A 30-foot ladder and a longer ladder are crossed in an alley. The longer one breaks just 20 feet from its foot and the top falls back to the other side of the alley and just touches the top of the 30-foot ladder. If the ladders cross just 10 feet above the ground, find the original length of the longer ladder. (This variation of the

old "crossed ladders" problem cost an aircraft company thousands of dollars in lost time during World War II by engineers and other technical people trying to solve it. I finally circulated a solution that probably saved the company thousands more, but alas, I received no credit for it.)



*624. *Proposed by Robert C. Gebhardt, Hopatcong, New Jersey.*

It is known and easy to prove that

$$\sum_{i=1}^{n} (i)(i!) = (n+1)! - 1.$$

Find a closed expression for $S(n)$ and prove that for $n > 1$, $S(n)$ is divisible by 3 where

$$S(n) = \sum_{i=1}^{n} i! = 1! + 2! + 3! + \ldots + n! .$$

625. *Proposed by Sam Pearsall, Loyola Marymount University, Los Angeles, California.*

Let G be a group in which there is a unique element x such that x generates a cyclic subgroup of order 2. Show that x commutes with every element of G.

Solutions

587. *[Spring 1985] Proposed by Morris Katz, Macwahoc, Maine.*

As a tribute to an Editor Emeritus of this department, find positive integers x and y, with $y > 2$, such that $x^y = BANKOFF$.

Solution by Robert C. Gebhardt, Hopatcong, New Jersey.

Assuming, as usual, that each letter stands for a different digit, and that there is no leading zero shown, then to obtain a seven-digit answer:

if y = 3, then 107 < x < 215; if y = 4, then 33 < x < 57;
if y = 5, then 16 < x < 26; if y = 6, then 10 < x < 15;
if y = 7, then 7 < x < 10; if y = 8, then 5 < x < 8;
if y = 9 or y = 10, then x = 5; and if y = 11, then x = 4.

By trying each possibility, skipping the many that would obviously not do the job, we get the only solution,

$$19^5 = 2476099.$$

Also solved by FRANK P. BATTLES and LAURA L. KELLEHER, Massachusetts Maritime Academy, Buzzards Bay, MARK EVANS, Louisville, KY, VICTOR G. FESER, Mary College, Bismarck, ND, JACK GARFUNKEL, Flushing, NY, RICHARD I. HESS, Rancho Palos Verdes, CA, JOHN M. HOWELL, Littlerock, CA, BOB LABARRE, United Technologies Research Center, East Hartford, CT, GLEN E. MILLS, Valencia Community College, Orlando, FL, HENRY J. OSNER, Modesto Junior College, CA, JOHN H. SCOTT, Macalester College, St. Paul, MN, W. R. UTZ, Rolla, MO, KENNETH M. WILKE, Topeka, KS, and the PROPOSER.

588. *[Spring 1985] Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, Pennsylvania.*

Find all solutions to the quadratic congruence

$$x^2 \equiv -1 \pmod{m}$$

where m is of the form $m = (rn \pm 1)^2 + r^2$.

Solution by Kenneth M. Wilke, Topeka, Kansas.

We shall use the identity

$$(U^2 + V^2)(A^2 + B^2) = (AU + BV)^2 + (BU - AV)^2$$

to solve the given congruence by making the right side of the identity equal to $x^2 + 1$ and $U^2 + V^2 = m$. Take $U = rn \pm 1$ and $V = r$. Then all solutions to $BU - AV = \pm 1$ are given by

$$A = n + (rn \pm 1)t \quad \text{and} \quad B = 1 + rt$$

where t is an arbitrary integer. Now take

$$x = \pm(AU + BV) = \pm[(rn \pm 1)\{n + (rn \pm 1)t\} + r\{1 + rt\}]$$
$$\equiv \pm[n(rn \pm 1) + r] \equiv \pm[r(n^2 + 1) \pm n] \pmod{m}.$$

It is easy to check that $x^2 + 1 \equiv 0 \pmod{m}$, so the solution to the given congruence is

$$x \equiv \pm[r(n^2 + 1) \pm n] \pmod{m}.$$

Also solved by the PROPOSER.

589. [Spring 1985] Proposed by Joyce W. Williams, University of Lowell, Massachusetts.

The integers 7, 3, and 10 are related by

$$7^3 = 3^5 + 10^2.$$

Is this the only set of positive integers that satisfies the relation

$$a^3 = b^5 + c^2?$$

Find all solutions.

Solution by C. C. Oursler, Southern Illinois University at Edwardsville.

Choose x to be any positive integer greater than 1 and let z be any positive integer such that $x^3 - z^5 = k$ is positive. Factor k into rs^2, where r is the square-free factor, i.e., $r = 1$ or has prime factors only to the first power. Multiply the above equation by r^{15} and we have the solution

$$(xr^5)^3 = (zr^3)^5 + (r^8s)^2.$$

More generally, we can multiply by w^{30}, where w is any positive integer, and get the general solution

$$(xr^5w^{10})^3 = (zr^3w^6)^5 + (r^8sw^{15})^2.$$

For each choice of $x > 1$, there is at least one suitable 3, hence a solution. Every solution is encountered since any given solution can be obtained from the formula above with $r = w = 1$.

A second solution was submitted by C. C. OURSLER. Partial solutions were submitted by ROBERT C. GEBHARDT, Hopatcong, NJ, RICHARD I. HESS, Rancho Palos Verdes, CA, JOHN M. HOWELL, Littlerock, CA, MASSACHUSETTS GAMMA, Bridgewater State College, MA, and the PROPOSER.

590. [Spring 1985] Proposed by Emmanuel O. C. Imonitie, Northwest Missouri State University, Maryville.

Find all solutions to the simultaneous equations

$$2^{x+y} = 6^y \quad \text{and} \quad 3^{x-1} = 2^{y+1}.$$

I. Solution by Henry S. Lieberman, Waban, Massachusetts.

Taking natural logarithms of the two given equations we get

$$(x + y)\ln 2 = y(\ln 2 + \ln 3) \quad \text{and} \quad (x - 1)\ln 3 = (y + 1)\ln 2,$$

$$(\ln 2)x - (\ln 3)y = 0 \quad \text{and} \quad (\ln 3)x - (\ln 2)y = \ln 6.$$

The unique solution to these simultaneous linear equations is

$$x = \frac{\ln 3}{\ln 3 - \ln 2} \quad \text{and} \quad y = \frac{\ln 2}{\ln 3 - \ln 2}.$$

Note that it does not matter to which base we take the logarithms since $(\log_r a)/(\log_r b) = (\log_s a)/(\log_s b)$ for any positive numbers a and b and any appropriate bases (positive numbers other than 1) r and s.

II. Solution by Bob Prielipp, University of Wisconsin-Oshkosh.

The first equation is equivalent to $2^x = 3^y$. Now multiply this equation and the second given equation side for side and simplify to yield

$$6^{x-1} = 8. \quad \text{Thus} \quad y = x - 1.$$

Now we have that $2^x = 3^{x-1}$, so

$$x = \frac{\ln 3}{\ln 3 - \ln 2}, \text{ whence } \quad y = \frac{\ln 2}{\ln 3 - \ln 2}.$$

Also solved by JAMES CAMPBELL, University of Missouri, Columbia, DAVID DELSESTO, North Scituate, RI, BRIAN DUBUIS and JOHN PUTZ, Alma College, MI, RUSSELL EULER, Northwest Missouri State University, Maryville, MARK EVANS, Louisville, KY, VICTOR G. FESER, Mary College, Bismarck, NO, JACK GARFUNKEL, Flushing, NY, ROBERT C. GEBHARDT (2 solutions), Hopatcong, NY, RICHARD I. HESS, Rancho Palos Verdes, CA, JOHN M. HOWELL, Littlerock, CA, Ralph King, St. Bonaventure University, NY, BOB LABARRE, United Technologies Research Center, East Hartford, CT, WARREN LEVINS, Greenville, SC, MASSACHUSETTS GAMMA, Bridgewater State College, GLEN E. MILLS, Valencia Community College, Orlando, FL, SAM PEARSALL, Loyola Marymount University, Los Angeles, CA, JOHN H. SCOTT, Macalester College, St. Paul, MN, HARRY SEDINGER, St. Bonaventure University, NY, WADE H. SHERARD, Furman University, Greenville, SC, W. R. UTZ, Columbia, MO, HAO-NHIEN QUI VU, Purdue University, West Lafayette, IN, KENNETH M. WILKE, Topeka, KS, and the PROPOSER. Partial solution by FRANK P. BATTLES, Massachusetts Maritime Academy, Buzzards Bay.

591. [Spring 1985] Proposed by Charles W. Trigg, San Diego, California.

Find all three-term arithmetic progressions of three-digit primes in the decimal system with first and last terms that are permutations of the same digit set and with only four consecutive digits involved in the three terms of each progression.

Solution by Kenneth M. Wilke, Topeka., Kansas.

Let p, q, and r be the three desired primes with $p < q < r$.

If p (hence also r) is formed from three distinct digits, then $r - p \equiv 0 \pmod 9$. Since p, q, and r are all primes, then $r - p \equiv 0 \pmod 4$. Hence $r - p \equiv 0 \pmod{36}$. Since only four consecutive digits a, $a + 1$, $a + 2$, and $a + 3$ are involved, then both a and $a + 3$ are found in both p and r. Of course, the other digit in p and r is either $a + 1$ or $a + 2$. Also, to give a solution, a prime must have a matching prime formed from a permutation of its digits. Primes of three distinct digits are *103*, ***241****, ***421****, *431*, *523*, ***463****, ***563****, ***643****, ***653****, ***457****, ***467****, ***547****, ***647****, ***587****, ***857****, and *967*. The starred primes have permutations that are also primes. From these pairs we get the solutions $(p, q, r) = (241, 331, 421)$ and $(467, 557, 647)$.

Clearly p must contain at least two distinct digits that differ by no more than *3*. Such primes containing exactly two digits are ***113****, ***131****, *211*, *223*, *233*, *311*, *313*, *433*, *443*, *353*, *557*, *577*, *677*, *757*, ***787****, ***877****, *887*, ***797****, ***977****, *997*, where starred primes have permutation mates. Here we find only the additional solution *(797, 887, 977)* which contains not four but just three consecutive digits.

Also solved by FRANK P. BATTLES, Massachusetts Maritime Academy, Buzzards Bay, VICTOR G. FESER, Mary College, Bismarck, ND, RICHARD I. HESS, Rancho Palos Verdes, CA, GLEN E. MILLS, Valencia Community College, Orlando, FL, JOHN H. SCOTT, Macalester College, St. Paul, MN, and the. PROPOSER.

592. [Spring 1985] *Proposed by Stanley Rabinowitz, Digital Equipment Cohp., Nashua, New Hampshire.*

Find all 2 by 2 matrices A whose entries are distinct non-zero integers such that for all positive integers n the absolute value of the entries of A are all less than some finite bound M.

Solution by Richard 1. Hess, Rancho Palos Verdes, California.

The eigenvalues of the given matrix

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

are

$$\lambda_{1,2} = \frac{a + d \pm \sqrt{(a - d)^2 + 4bc}}{2}.$$

For all elements of A^n to be bounded we must have $|\lambda_i| \leq 1$ for $i = 1$ and *2*.

If $a + d = 0$, then $\lambda_{1,2} = \pm\sqrt{bc - a^2}$, which implies that $bc = a^2$ or $a^2 - 1$ or $a^2 + 1$. If $a + d = \pm 1$, then

$$\lambda_{1,2} = \frac{1}{2}(\pm 1 \pm \sqrt{(2a \mp 1)^2 + 4bc}),$$

which implies that $bc = -a(a \mp 1)$ or $-a(a \mp 1) - 1$.

Also partially solved by the. PROPOSER.

593. [Spring 1985] *Proposed by Joe. Van Austin, Emory University, Atlanta, Georgia.*

Russian roulette is played with a gun having n chambers, in which k bullets are placed at random $(0 < k < n)$. Find the expected number of tries until the first bullet is fired if the chambers are spun

(i) before each shot.

(ii) only before the first shot.

Solution by John M. Howell, Littlerock, California.

(i) The probability of firing the first shot on try x is

$$P(x) = (1 - \frac{k}{n})^{x-1}(\frac{k}{n}); \quad x = 1, 2, 3, \ldots$$

and the expected number of tries is given by

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

(ii) Here we have

$$P(x) = (\frac{n - k}{n})(\frac{n - k - 1}{n - 1})\ldots(\frac{n - k - x + 2}{n - x + 2})(\frac{k}{n - x + 1})$$

$$= \frac{k(n - k)!(n - x)!}{n!(n - k - x + 1)!}; \quad x = 1, 2, \ldots, n - k + 1.$$

For k = *1* this yields $P(x) = 1/n$ for $x = 1, 2, \ldots, n$. When k = *2* we have $P(x) = 2(n - x)/n(n - 1)$ for $x = 1, 2, \ldots, n - 1$. For $k = 3$, $P(x) = 3(n - x)(n - x - 1)/n(n - 1)(n - 2)$ for $x = 1, 2, \ldots, n - 2$, etc.

Now the expected number of trials to the first shot is calculated for each k. For $k = 1$ we get that

$$E = \sum_{x=1}^{n} \frac{x}{n} = \frac{n(n+1)}{2n} = \frac{n+1}{2}.$$

For $k = 2$ we have

$$E = \sum_{x=1}^{n-1} \frac{2x(n-x)}{n(n-1)} = \frac{2}{n(n-1)}\left[\frac{n^2(n-1)}{2} - \frac{n(n-1)(2n-1)}{6}\right]$$

$$= n - \frac{2n-1}{3} = \frac{n+1}{3},$$

and so forth. In general, E $\frac{n+1}{k+1}$

Also solved by RICHARD I. HESS, Rancho Palos Verdes, CA, HENRY S. LIEBERMAN, Waban, MA, HARRY SEDINGER, St. Bonaventure University, NY, and the PROPOSER. One incorrect solution was received.

594. [Spring 1985] *Proposed by* R. S. Luthar, University of Wisconsin Center, Janesville.

Prove that

$$\int_0^1 x^x \ln x\,dx = -\int_0^1 x^x\,dx.$$

Solution by Jack Garfunkel, Flushing, N w York.

Equivalently we show that

$$\int_0^1 x^x(1 + \ln x)\,dx = \int_1^1 du = u\Big]_1^1 = 0,$$

where $u = x^x$, since $\lim_{x\to 0} x^x = 1$. The given equation follows.

Also solved by EDWARD S. ARISMENDI, JR., California State University, Long Beach, FRANK P. BATTLES, Massachusetts Maritime Academy, Buzzards Bay, BARRY BRUNSON, Western Kentucky University, Bowling Green, RUSSELL EULER, Northwest Missouri State University, Maryville, MARK EVANS, Louisville, KY, ROBERT C. GEBHARDT, Hopatcong, NJ, RICHARD I. HESS, Rancho Palos Verdes, CA, RALPH KING, St. Bonaventure University, NY, BOB LABARRE, United Technologies Research Center, East Hartford, CT, HENRY S. LIEBERMAN, Waban, MA, PETER A. LINDSTROM, University of Wisconsin Center, Janesville, BOB PRIELIPP, University of Wisconsin-Oshkosh, JOHN PUTZ, Alma Cortege, MI, JOHN H. SCOTT, Macalester College, St. Paul, MN, HARRY SEDINGER, St. Bonaventure University, NY, WADE H. SHERARD, Furman University, Greenville, SC, VIS UPATISRIMGA, Humboldt State University, Arcata, CA, HAO-NHIEN QUI VU, Purdue University, West Lafayette, IN, and the PROPOSER.

595. [Spring 1985] *Proposed by* Harry Herein, Livermore, California.

If the integers from 1 to 5000 are listed in equivalence classes according to the number of written characters (including blanks and hyphens) needed to write them out in full in correct English, there are exactly forty such nonempty classes. For example, class "4" contains 4, 5, and 9, since FOUR, FIVE, and NINE are the only such numbers that can be written out with exactly four characters. Similarly, class "42" contains 3373, 3377, 3378, 3773, 3777, 3778, 3873, 3877, and 3878. Find the unique class "n" that contains just one number.

Solution by Bob LaBarre, United Technologies Research Center, East Hartford, Connecticut.

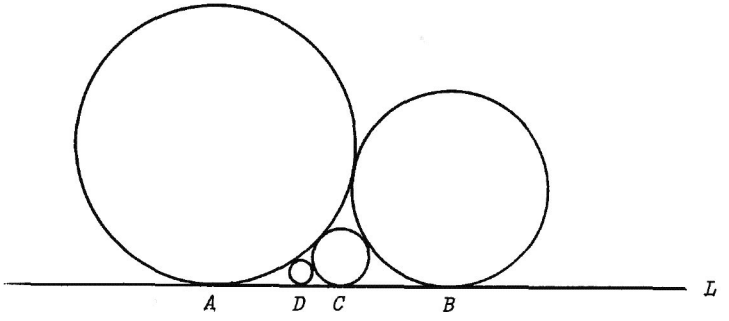
First note that, of the nine nonzero digits, 3 require 3 characters, 3 require 4 characters, and 3 require 5 characters. Additionally, only the number 17 (9 characters) has a unique representation for numbers less than 20. But 42 also uses 9 characters. Consequently, the last digit of the unique number in class "n" must be a zero (using no characters). The tens digit is also zero since 10 uses 3 characters (as does 01), 20, 30, 80 and 90 use 6 characters, and 40, 50 and 60 require 5. The number 70 uses 7 characters, but so also does 15. The above discussion for the units digit also applies to the hundreds digit, so it too is zero. Therefore, uniqueness has implied that the number is 1000, 2000, 3000, 4000, or 5000. Again uniqueness implies that the number is 3000 and the class is "14".

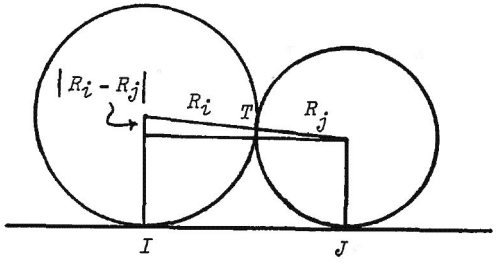
Also solved by FRANK P. BATTLES and LAURA L. KELLEHER, Massachusetts Maritime Academy, Buzzards Bay, MARK EVANS, Louisville, KY, VICTOR G. FESER, Mary College, Bismarck, ND, RICHARD I. HESS, Rancho Palos Verdes, CA, GLEN E. MILLS, Valencia Community College, Orlando, FL, JOHN H. SCOTT, Macalester Cottage., St. Paul, MN, and the PROPOSER.

596. [Spring 1985] *Proposed by* Stanley Rabinowitz, Digital Equipment Corp., Nashua, New Hampshire.

Two circles are externally tangent and tangent to a line L

at points A and B. A third circle is inscribed in the curvilinear triangle bounded by these two circles and L and it touches L at point C. A fourth circle is inscribed in the curvilinear triangle bounded by line L and the circles at A and C and it touches the line at D. Find the relationship between the lengths AD, DC, and CB.





Solution by Harry Sedinger, St. Bonaventure University, St. Bonaventure, New Yolk.

Consider two circles with radii R_i and R_j, each tangent to a line at points I and J respectively and tangent externally to each other at point T. The segment connecting the centers also contains point T, has length $R_i + R_j$, and is the hypotenuse of a right triangle with legs of length $|R_i - R_j|$ and IJ. Thus

$$(R_i + R_j)^2 = (R_i - R_j)^2 + (IJ)^2,$$

which yields

$$IJ = 2\sqrt{R_i R_j}\ .$$

Now we have that

$$AD \cdot CB = 2\sqrt{R_A R_D} \cdot 2\sqrt{R_C R_B} = 2\sqrt{R_D R_C} \cdot 2\sqrt{R_A R_B} = DC \cdot AB.$$

Thus we have

$$AD \cdot CB = DC \cdot AB \quad \text{or equivalently} \quad AD \cdot CB = DC(AD + DC + CB).$$

Also solved by MARK EVANS, *Louisville, KY,* RICHARD I. HESS, *Rancho Palos Verdes, CA,* JOHN M. HOWELL, *Littlerock, CA,* RALPH KING, *St. Bonaventure University, NY,* HENRY S. LIEBERMAN, *Waban,* MA, NORTHWEST MISSOURI STATE UNIVERSITY MATHEMATICS CLUB, *Maryville,* STEPHANIE SLOYAN, *Georgian Court College, Lakewood, NJ,* JOHN H. SCOTT, *Macalester College,* St. *Paul, MN, and the.* PROPOSER.

597. [Spring 1985] *Proposed by Stanley Rabinowitz, Digital Equipment Coup., Nashua, New Hampshire.*

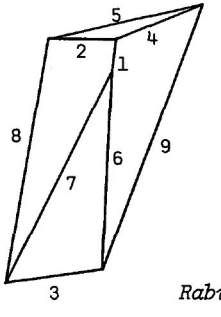
Find the smallest n such that there exists a polyhedron of non-zero volume and with n edges of lengths 1, 2, 3, ..., n.

I. Solution by the proposer.

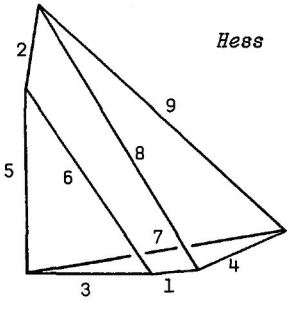
The edge of length 1 must appear in two faces. Neither face can be a triangle since the sides are integral and would have to differ by less than 1. Thus the smallest number of sides these two faces can have is 4 each, which yields a polyhedron of 9 edges. Such a polyhedron exists, as shown in the sketch, so $n = 9$.

II.. Solution by Richard I. Hess, Rancho Palos Verdes, California.

The best I can do is $n = 9$. See the figure.



Rabinowitz



Hess

The two solutions are each topologically equivalent to a triangular prism and were drawn from wire models.

598. [Spring 1985] **Proposed by Gregory Wulczyn, Bucknell University, Lewisburg, Pennsylvania.**

Establish the formula

$$D^n(e^{rx}\cos ax) = e^{rx}\cos ax\left[r^n - \binom{n}{2} r^{n-2}a^2 + \binom{n}{4} r^{n-4}a^4 - \cdots\right]$$

$$+ e^{rx}\sin ax\left[-\binom{n}{1} r^{n-1}a + \binom{n}{3} r^{n-3}a^3 - \binom{n}{5} r^{n-5}a^5 + \cdots\right]$$

and find the corresponding formula for

$$D^n(e^{rx}\sin ax).$$

Solution by **Frank P. Battles, Massachusetts Maritime** Academy, **Buzzards** Bay.

Euler's identity states that

$$e^{rx}(\cos ax + i\sin ax) = e^{(r+ia)x}$$

where $i^2 = -1$. Hence we have

$$D^n[e^{rx}(\cos ax + i\sin ax)] = (r+ia)^n e^{(r+ia)x}$$

$$= \sum_{j=0}^{n} \binom{n}{j} r^{n-j}(ia)^j e^{rx}(\cos ax + i\sin ax).$$

Equating the real parts of this equation yields the stated result. Equating the imaginary coefficients gives

$$D^n(e^{rx}\sin ax)$$

$$= e^{rx}\cos ax\left[r^{n-1}a - \binom{n}{3} r^{n-3}a^3 + \binom{n}{5} r^{n-5}a^5 - \cdots\right]$$

$$+ e^{rx}\sin ax\left[r^n - \binom{n}{2} r^{n-2}a^2 + \binom{n}{4} r^{n-4}a^4 - \cdots\right].$$

Also solved by RUSSELL EULER, **Northwest Missouri State University, Maryville,** MARK EVANS, **Louisville,** KY, RICHARD I. HESS, Rancho **Palos Verdes,** CA, JOHN H. SCOTT, **Macalester** Cortege., **St. Paul,** MN, VIS UPATISRINGA, **Humboldt** State **University, Arcata,** CA, **HAO-NHIEN** QUI **VU, Purdue University, West Lafayette,** IN, and the. PROPOSER.

599. [Spring 1985] **Proposed jointly by Gregg Patruno, Princeton University, New** Jersey, and **Murray S.** Klamkin, **University of** Alberta, Edmonton, Canada.

Prove that

$$\frac{\sin^2 x\cos^2 y}{\cot^2 x\cot^2 y} = \frac{\cos^2 x - \cos^2 y}{\cot^2 x - \cot^2 y}$$

and generalize this result by finding under what conditions on functions f and g it is true that

$$\frac{f(x)\cdot f(y)}{g(x)\cdot g(y)} = \frac{f(x) - f(x)}{g(x) - g(y)}.$$

Solution by Hao-Nhien Qui Vu, **Purdue University,** West **Lafayette, Indiana.**

Consider the generalization, where $g(x) \neq 0$. Clearly this equation is satisfied if $f(x) = 0$ for all x. Otherwise the equation is equivalent to

$$\frac{1}{g(x)} - \frac{1}{g(y)} = \frac{1}{f(x)} - \frac{1}{f(y)},$$

and finally to

$$\frac{1}{g(x)} - \frac{1}{f(x)} = \frac{1}{g(y)} - \frac{1}{f(y)}.$$

This equation is satisfied if and only if each side is a constant.

Conversely, if we have either

$$f(x) = 0 \text{ for all } x \quad \text{or} \quad \frac{1}{f(x)} = \frac{1}{g(x)} - C,$$

then the above argument reverses to prove the stated equation.

Since

$$\frac{1}{\cos^2 x} - \frac{1}{\cot^2 x} = \sec^2 x - \tan^2 x = 1,$$

a constant, the first stated equation is true whenever the denominators are nonzero.

Also solved by FRANK P. BATTLES, **Massachusetts Maritime** Academy, Buzzard* Bay, RUSSELL EULER, **Northwest Missouri State University,** Maryville, RICHARD I. HESS, Rancho **Palos Verdes,** CA, and the. PROPOSER. Partial **solutions were submitted** by VICTOR G. FESER, **Mary College, Bismarck,** ND, RALPH KING, St. **Bonaventure University, NY,** BOB **LABARRE,** United **Technologies Research Center,** East **Hartford,** CT, JOHN H. SCOTT, **Macalester College, St. Paul,** MN, and VIS UPATISRINGA, **Humboldt** State **University, Arcata,** CA.

The Perfect Problem Solver - by the Late Roger Kuehl.

To become the perfect problem solver you will need a combination of, Logic and flair. You must be hound or brilliant HA the occasion demands. You must be able to draw the right inference from the problem statement, visualize all the. possibilities and grasp what the. proposer is flying to say, often before on. better than he actually does it, in order to select the. most promising approach. On top of, this you still need to know what others in the past have done with the same or similar problems and how they have been historically approached and be prepared to collaborate with others.

Which makes the whole thing impossible!

Editor's Note - Rogm Kuehl was a highway engineer who took great interest in the. Problem Department of, the Journal.

✻

On a letter to the Editor:

A letter to the. Editor which was published in the Spring 1984 issue of, the Journal contained some unfortunate omissions of, symbols and other typographical errors. The titter. which follows was in response to an inquiry directed to the letterwriter by the current Editor.

Dear Editor:

If I remember correctly, my previous statement was:

If $a \geq 1$ and $b > 1$, then $\tan^{-1} a + \tan^{-1} b + \tan^{-1} \frac{a+b}{ab-1} = \pi$.

However, the one that I give now is still more general: If a and b are positive and ab > 1, then (the same equality holds).

_____'s result follows as a corollary to my new statement. The proof of my new statement (omitted here, Ed.) is given on the next page.

Sincerely,
R. S. Luthar
University of Wisconsin
Janesville

✻

TECHNO=LOGOGRIPHIA

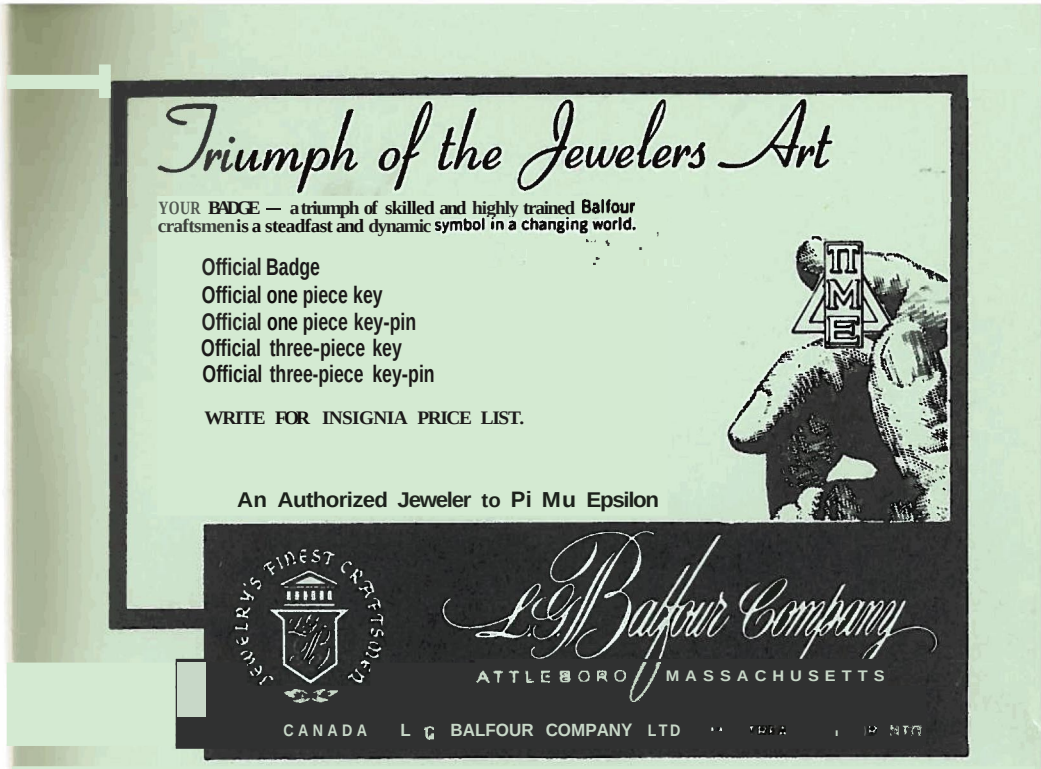
Anacrostic Puzzles for Scientists, Technologists, and Engineers. Texts are selected from the literature of science and technology, fact and fiction. About half the clue words are chosen from the biography and terminologies of science and technology.

COMPUCROSTICS™

Anacrostic puzzles on disks. The entire solution process takes place on the screen of your computer.

Write to

Robert Forsberg
P. O. Box 281
Lexington, MA 02173



PI MU EPSILON JOURNAL PRICES

PAID IN ADVANCE ORDERS:

Members:	**$ 8.00 for 2 years** **$20.00 for 5 years**
Non-Members:	**$12.00 for 2 years** **$30.00 for 5 years**
Libraries:	**$30.00 for 5 years (same as non-members)**
Back Issues	**$ 4.00 per issue**
Complete volume	**$30.00 (5 years, 10 issues)**
All issues	**$210.00 (7 complete back volumes plus current volume subscription)**