How few radii?
Problem 1041

The ΠΜΕ Journal

Volume 11, Number 6
Spring 2002
A CYCLOTOMIC DETERMINANT

AYOUB B. AYOUB*

In this article, we will evaluate an interesting determinant whose entries are related to equally spaced points on the unit circle, hence the name cyclotomic determinant. We denote the determinant whose order is \( \frac{p-1}{2} \) by \( \Delta_p \), where

\[
\Delta_p = \begin{vmatrix}
1 & \cos \frac{2\pi}{p} & \cos \frac{4\pi}{p} & \cdots & \cos \frac{(p-2)\pi}{p} \\
1 & \cos \frac{3\pi}{p} & \cos \frac{5\pi}{p} & \cdots & \cos \frac{(p-3)\pi}{p} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \cos \frac{(p-1)\pi}{p} & \cos \frac{(p-3)\pi}{p} & \cdots & \cos \frac{(p-1)(p-3)\pi}{2p}
\end{vmatrix}
\]

and \( p \) is an odd prime number.

We will show that the absolute value of this determinant is \( \frac{p}{4} e^{\pi^2/4} \). The reader may try to verify the following two special cases:

\[
\begin{vmatrix}
1 & \cos \frac{2\pi}{5} & \cos \frac{4\pi}{5} \\
1 & \cos \frac{4\pi}{5} & \cos \frac{8\pi}{5} \\
1 & \cos \frac{6\pi}{5} & \cos \frac{12\pi}{5}
\end{vmatrix} = \frac{-\sqrt{5}}{2} \quad \text{and} \quad \begin{vmatrix}
1 & \cos \frac{2\pi}{7} & \cos \frac{4\pi}{7} & \cos \frac{6\pi}{7} \\
1 & \cos \frac{2\pi}{7} & \cos \frac{4\pi}{7} & \cos \frac{6\pi}{7} \\
1 & \cos \frac{2\pi}{7} & \cos \frac{4\pi}{7} & \cos \frac{6\pi}{7}
\end{vmatrix} = \frac{7}{4}
\]

Now, we will proceed with the proof. First we will express each entry in terms of \( \omega \), a primitive \( p'th \) root of unity, i.e., \( \omega^p = 1 \) while \( \omega^r \neq 1 \) for \( r < p \). Then \( \omega \) satisfies the cyclotomic equation \( \omega^{p-1} + \omega^{p-2} + \omega^{p-3} + \cdots + 1 = 0 \), \( [1] \). If we consider \( \omega = e^{2\pi p i / p} + i \sin \frac{2\pi}{p} \), then \( \cos \frac{2\pi}{p} = \frac{1}{2}(\omega + \omega^{-1}) \), and \( \cos \frac{4\pi}{p} = \frac{1}{2}(\omega^2 + \omega^{-2}) \).

Using these notations, the cyclotomic determinant \( \Delta_p \) takes the form

\[
\begin{vmatrix}
1 & \frac{1}{2}(\omega + \omega^{-1}) & \frac{1}{2}(\omega^2 + \omega^{-2}) & \cdots & \frac{1}{2}(\omega^{p-1} + \omega^{-1}) \\
1 & \frac{1}{2}(\omega + \omega^{-1}) & \frac{1}{2}(\omega^2 + \omega^{-2}) & \cdots & \frac{1}{2}(\omega^{p-1} + \omega^{-1}) \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \frac{1}{2}(\omega^{p-1} + \omega^{-1}) & \frac{1}{2}(\omega^{p-1} + \omega^{-1}) & \cdots & \frac{1}{2}(\omega^{p-1} + \omega^{-1})
\end{vmatrix}
\]

but then

\[
\Delta_p = \frac{1}{2} e^{\pi^2/4} \text{A}
\]

where

\[
\text{A} = \begin{vmatrix}
\omega + \omega^{-1} & \omega^2 + \omega^{-2} & \cdots & \omega^{p-2} + \omega^{-p+2} \\
\omega^2 + \omega^{-2} & \omega^4 + \omega^{-4} & \cdots & \omega^{p-4} + \omega^{-p+4} \\
\omega^3 + \omega^{-3} & \omega^6 + \omega^{-6} & \cdots & \omega^{p-6} + \omega^{-p+6} \\
\vdots & \vdots & \ddots & \vdots \\
\omega^{p-1} + \omega^{-1} & \omega^{p-1} + \omega^{-1} & \cdots & \omega^{p-1} + \omega^{-1}
\end{vmatrix}
\]

*The Pennsylvania State University, Abington College
To evaluate the determinant \( A \), we will consider a larger determinant \( B \) of order \( \frac{p+1}{2} \) where

\[
B = \begin{vmatrix}
1 & 2 & \cdots & 2 \\
\omega + \omega^{-1} & \omega^2 + \omega^{-2} & \cdots & \omega^p + \omega^{-p} \\
\omega^2 + \omega^{-2} & \omega^4 + \omega^{-4} & \cdots & \omega^{p+1} + \omega^{-(p+1)} \\
\omega^3 + \omega^{-3} & \omega^6 + \omega^{-6} & \cdots & \omega^{p+2} + \omega^{-(p+2)} \\
& \cdots & \cdots & \cdots \\
1 & \omega^{p-1} + \omega^{-(p-1)} & \omega^{p+1} + \omega^{-(p+1)} & \cdots & \omega^{p+2} + \omega^{-(p+2)}
\end{vmatrix}
\]

Now we will evaluate \( B^2 \) in two different ways from which we will get \( |A| \). To that end, we will need the following:

Since \( \omega^p + \omega^{-p} = \omega^q + \omega^{-q} \) is also a residue system modulo \( p \), then dividing by \( \omega^p - 1 \), we get \( \sum_{i=1}^{(p-1)/2} (\omega^i + \omega^{-i}) + 1 = 0 \). And because \( 1, 2, 3, \ldots, (p-1) \) is a residue system modulo \( p \), then \( x, 2x, 3x, \ldots, (p-1)x \) is also a residue system modulo \( p \), assuming that \( x \neq 0 \mod p \), (see [2]). Consequently,

\[
\sum_{i=1}^{(p-1)/2} (\omega^i + \omega^{-i}) + 1 = 0.
\]

If we multiply \( B \) by itself, the result is:

\[
B^2 = \begin{vmatrix}
p & 0 & 0 & \cdots & 0 \\
0 & p & 0 & \cdots & 0 \\
0 & 0 & p & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & 0 & \cdots & p
\end{vmatrix} = p^{(p+1)/2}
\]

That is because the entries \( a_{(x+1)(y+1)} \) of \( B^2 \), with each \( x \) and \( y \) assuming the values \( 0, 1, 2, \ldots, \frac{p+1}{2} \), are calculated as follows:

1. When \( x = y = 0 \),

\[
a_{11} = 1 + 2 \left( \frac{p-1}{2} \right) = p.
\]

2. When \( x = 0, y \neq 0 \),

\[
a_{1(y+1)} = 2 + 2 \sum_{i=1}^{(p-1)/2} (\omega^i + \omega^{-i}) = 2 + 2(-1) = 0,
\]

3. When \( x \neq y \neq 0 \),

\[
a_{(x+1)(y+1)} = 2 \sum_{i=1}^{(p-1)/2} (\omega^{x+i} + \omega^{-x-i})^2 = 2 + \sum_{i=1}^{(p-1)/2} (\omega^{2x+i} + \omega^{-2x-i} + 2).
\]

Hence \( a_{(x+1)(y+1)} = 2 + (-1) + 2 \left( \frac{p+1}{2} \right) = p \); and

A CYCLOTOMIC DETERMINANT

4. When \( 0 \neq x \neq y \neq 0 \),

\[
a_{(x+1)(y+1)} = 2 + \sum_{i=1}^{(p-1)/2} (\omega^{xt} + \omega^{-x-y}) (\omega^{yt} + \omega^{-x-y})
\]

\[
= 2 + \sum_{i=1}^{(p-1)/2} (\omega^{(x+y)t} + \omega^{-xt}) + \sum_{i=1}^{(p-1)/2} (\omega^{(x+y)t} + \omega^{-xt})
\]

Thus \( a_{(x+1)(y+1)} = 2 + (-1) + (-1) = 0 \).

Now we go back to \( B \) and add all the columns to the last one to get

\[
B = \begin{vmatrix}
1 & 2 & \cdots & 2 & p \\
1 & \omega + \omega^{-1} & \omega^2 + \omega^{-2} & \cdots & \omega^p + \omega^{-p} \\
1 & \omega^2 + \omega^{-2} & \omega^4 + \omega^{-4} & \cdots & \omega^{p+1} + \omega^{-(p+1)} \\
1 & \omega^3 + \omega^{-3} & \omega^6 + \omega^{-6} & \cdots & \omega^{p+2} + \omega^{-(p+2)} \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
1 & \omega^{p-1} + \omega^{-(p-1)} & \omega^{p+1} + \omega^{-(p+1)} & \cdots & \omega^{p+2} + \omega^{-(p+2)}
\end{vmatrix}
\]

Therefore \( B = pA \) and so \( B^2 = p^2 A^2 \). If we use (2), we get \( p^{(p+1)/2} = p^2 A^2 \) from which \( A^2 = p^{(p-3)/2} \). Thus \( |A| = p^{(p-3)/4} \). But (1) implies that \( |\Delta_p| = (\frac{1}{2})^{(p-3)/2} |A| \).

Hence

\[
|\Delta_p| = \left( \frac{1}{2} \right)^{\frac{p+1}{2}} p^{\frac{p-3}{2}} = \left( \frac{p}{4} \right)^{\frac{p-3}{4}}.
\]

A byproduct of the previous proof is the following result: If we denote the underlying matrix of the determinant \( B \) by \( M \), then equation (2) implies that \( M^2 = pI \), where \( I \) is the \( \frac{p+1}{2} \) by \( \frac{p+1}{2} \) identity matrix. But this means that \( M/\sqrt{p} \) is a square root of \( I \).

REFERENCES


Ayoub B. Ayoub, The Pennsylvania State University, Abington College, Abington, PA 19001

Ayoub B. Ayoub received his Ph.D. in algebraic number theory from Temple University in 1980. He has published extensively on a variety of topics from college mathematics and is an active contributor to our problem department.
THE MATHEMATICAL ASSOCIATION OF AMERICA

Advancing Mathematics Education, primarily at the collegiate level

Some of the benefits of membership include:


Publications - Focus Newsletter, Math Horizons Magazine

MAA books

MAA Section Membership

Professional Enhancement Programs

Joint the MAA today at a special introductory price
(New members only)

For More Information:

WWW.MAA.ORG  800-331-1622

Abstract. In the course of some of Frank Morley's other geometrical researches around the turn of the century, a rather surprising special case of a more general result, now known as Morley's theorem, appeared: The three (appropriately chosen) intersections of the internal angle trisectors of a triangle form an equilateral triangle. After a short and incomplete look at who Frank Morley was, we will then look at three geometrical proofs of this most spectacular theorem.

1. Frank Morley. Frank Morley was born September 9th, 1860, in Woodridge, Suffolk, England. Morley entered King's College Cambridge in 1879, where he studied mathematics. He graduated with a B.A. in 1884. After teaching for three years at Bath College in England, he moved to the United States. He found work as an instructor at Quaker College, Haverford, Pennsylvania. At Haverford, he was quickly promoted to professor. Around 1900 he moved to Johns Hopkins University to head their mathematics department. Morley was the President of the American Mathematical Society from 1919 to 1920, and the editor of the American Journal of Mathematics from 1900 to 1921 [3] [7] [6].

Frank Morley was known mostly for his work in geometry. But he was also an avid problem proposer, and over the course of fifty years he published over 60 mathematical problems in the Educational times. He was also a superb chess player, even beating the algebraist Lasker on one occasion, who was then the World Chess Champion. Frank Morley died at the age of 77 on October 17th 1937 in Baltimore, Maryland [3] [7].

2. Morley's Triangle. Morley's theorem is implicit in the many general theorems of Morley's paper of 1900 "On the Metric Geometry of the Plane n-line" which appeared in the first issue of the Transactions of the American Mathematical Society [4] [6]. Morley's theorem has spawned many proofs and generalizations. For some one hundred and fifty references see [6].

When I first heard of Morley's theorem, I was overcome with excitement. Anyone who appreciates beautiful theorems, especially those of a geometric nature, will see why this jewel of elementary geometry has intrigued so many.

THEOREM 1 (Morley). The three (appropriately chosen) intersections of the internal angle trisectors of a triangle form an equilateral triangle.

" Appropriately chosen" means: If the triangle has vertices A, B, and C, choose the intersection of the trisectors at A and B that lies nearest side AB, the intersection of the trisectors at B and C that lies nearest side BC, and the intersection of the trisectors at A and C that lies nearest side AC.

3. Proofs. We will now look at three different proofs of Morley's theorem. You may find one clearer or more appealing than the others. The three proofs will use basic geometric techniques. It should be noted that Morley's theorem is still true for the exterior angle trisectors of a triangle — for example see [8].

The following proof is due to H.D. Grossman and can be found in original form in [2]. The approach taken is to begin with an arbitrary triangle, then, by choosing points and angles and constructing lines, construct a triangle, which we finally show is in fact the Morley triangle.
Proof. Let a triangle $ABC$ have interior angles $3a, 3b,$ and $3c$ at $A, B,$ and $C$ respectively. On the angle trisectors at $B$ and $C$, we pick points $D, E, F, H,$ and $K$ as shown, and as explained in the following text. The point $D$ is the intersection of the lines $s$ and $n$ equals $180^\circ - (180^\circ - (a + c)) - c = a$. The lines $m$ and $n$ meet at $A$, hence meet at an angle $3a$.

Now all we need to do to complete the proof is to show that the lines $m, n, r,$ and $s$, meet at a point. The line $KF$ joins the vertices of two isosceles triangles ($\triangle DKE$ and $\triangle DFE$) and therefore bisects $\angle DKE$. Then in the triangle formed by the lines $m, n,$ and the points $B, K$, the angle bisector of the angle of intersection of the lines $m$ and $s$ passes through $F$, since the angle bisectors of a triangle always meet at a point. Since this bisector is parallel to the line $r$, it coincides with it. A similar argument works for the line $s$ in the triangle formed by the lines $r, n$ and the points $H, C$. Thus we conclude from the preceding that the lines $m, n, r,$ and $s$ meet at a point.  

The next proof will look at is one given by D.J. Newman in [5]. The proof works by using data from the given triangle to start with an equilateral triangle and build what turns out to be a triangle that is similar to the given one, and its internal angle trisectors. The main tool used in the proof is the law of sines.

Proof. In this proof we will switch to radians for angle measure. Let $a, b,$ and $c$ be the interior angles of an arbitrary nondegenerate triangle $T$. Draw an equilateral $\triangle PQR$, which we normalize to have side length 1. Construct the points $A, B,$ and $C$ using $a, b,$ and $c$ to direct rays outward from the vertices of $\triangle PQR$, in the manner shown in the diagram.

Apply the law of sines to $\triangle AQR$ to get

$$\frac{AR}{\sin[(c+\pi)/3]} = \frac{1}{\sin(a/3)}$$

So

$$AR = \frac{\sin[(c+\pi)/3]}{\sin(a/3)}$$

Applying the law of sines to $\triangle BPR$ gives

$$\frac{BR}{\sin[(c+\pi)/3]} = \frac{1}{\sin(b/3)}$$
MORLEY'S TRIANGLE

So

$$BR = \frac{\sin \left( \frac{(c + \pi)/3}{2} \right)}{\sin \left( \frac{b/3}{2} \right)}.$$ 

Also \(<ARB = 2\pi - (a + \pi)/3 - (b + \pi)/3 - \pi/3 = (c + 2\pi)/3>.

Thus we know two sides of \(\triangle ARB\) and the included angle, so the two remaining angles are determined, and they must be \(a/3\) and \(b/3\), at the points \(A\) and \(B\) respectively. One can verify this using the law of sines.

![Diagram of Morley's Triangle]

Now a similar procedure can be carried out to determine the unknown angles for \(\triangle BPC\) and \(\triangle CQA\). We then see that they are the angle trisectors of \(<A, <B, \text{ and } <C\) from the given equilateral triangle. Now take \(\triangle PQR\) and \(\triangle ABC\) and scale by an appropriate scale factor to get a scaled \(\triangle ABC\) which is congruent to our original \(\triangle\). The resulting scaled \(\triangle PQR\) is still equilateral, and is the Morley triangle of the original \(\triangle\).

The last proof we will look at is a bit more involved than the previous theorems, but I believe that you will feel a sense of satisfaction after going through this proof. We have seen three geometric proofs of Morley’s theorem of varying difficulty. If you are interested, you can find proofs that use different techniques, such as proofs heavy in trigonometry, proofs that use complex numbers, or that use projective geometry. A good place to look for references to such proofs is in the list of references given in \([6]\).

The fact that Morley’s theorem was only found in the early part of this century, even after millennia of work in plane geometry, leads one to wonder if there are still many simple and beautiful results of plane geometry that are still hidden. Will you be the next person to find a most beautiful geometrical theorem?

Acknowledgments. I would like to thank Richard Ganong for his helpful suggestions.

REFERENCES


From the Right Side

How to Learn

While trying to learn some knowledge or lore
Enjoying yourself I truly confess
Has never been proven to teach anymore
But never suspected of teaching you less
In fact you may also learn other things
The pleasure of hearing your heart as it sings

Donald Moiseevich Solitar

Donald Solitar, Professor of Mathematics at York University, is the author, along with Wilhelm Magnus and Abraham Karrass, of "Combinatorial Group Theory", the classic text in that subject. Besides being a member of IIME, he is a Fellow of the Royal Society of Canada, and a recipient of the Ontario Teaching Award.

This poem appeared in his "Reason, Rhyme and Rhythm: A Fight against Fashion". There is no punctuation throughout the volume, not even in the entry entitled "A Fat and Kind Professor".

The IIME Journal invites those of you who paint, draw, compose, or otherwise use the other side of your brains to submit your mathematically inspired compositions.

1. Introduction. In this paper, we generalize results reported in [3]; and, as is done there, we introduce this circle of ideas by reminding the reader of the well-known HATCHECK PROBLEM: Let $S_n$ denote the group of all permutations of the set $[n] = \{1, \ldots, n\}$. If an element $a$ is chosen uniformly at random from $S_n$, what is the probability $P_n$ that $a$ will have no fixed points? Also, what is the limit $\lim_n P_n$?

The answer to this problem is part of the folklore of mathematics and may be found in any introductory combinatorics text (e.g. [1]). This paper treats some extensions of this problem, which are quite natural, provided one views the Hatcheck Problem as a question about the disjoint cycle factorization (or DCF) of a permutation $\sigma$. We will explain the DCF, which is for many purposes the most useful way to specify $\sigma$, by means of an example; a more complete and formal discussion may be found in [2].

Suppose that a class with eight students holds a pollyanna. Each student draws the name of a student out of a hat. This determines the "pollyanna permutation" $\sigma$ of the eight students; if student $i$ draws the name of student $a(i)$, then $i$ must buy a present for $a(i)$. For the purposes of this example, we must allow the possibility that a student might draw his or her own name (i.e., that $a(i) = i$), although this would be rather strange for a pollyanna.

A cycle of $\sigma$ is now obtained by choosing a student, asking whose name she has, then going to that student and asking whose name he has, and proceeding this way until you get back to the original student. Of course, when you get back to the first person, there will very likely be people you have not included; these people belong to other cycles, and the list of all of these cycles is the DCF of $\sigma$. Thus, if $\sigma$ is given by the array

$$
\begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
2 & 6 & 3 & 7 & 8 & 5 & 4 & 1
\end{pmatrix}
$$

then 1 must buy a present for 2, who must buy one for 6, who must buy one for 5, who must buy one for 8, who must buy one for 1. This is one cycle of the permutation $\sigma$:

$$
1 \rightarrow 2 \rightarrow 6 \rightarrow 5 \rightarrow 8 \rightarrow 1,
$$

which is usually indicated simply $(12658)$. (This is called a 5 cycle, since it includes five people.) The other two cycles of $\sigma$ are the 2 cycle $(47)$, since these two students must exchange presents, and the 1 cycle $(3)$, since person 3 must buy a present for him/herself. The complete DCF of $\sigma$ is the list of all three of these cycles:

$$
\sigma = (12658)(47)(3).
$$

*benefice University. Ms. Corp's work was supported by HHMI and by the Luce Foundation for Women in Science Scholars Program at Benedictine University. HHMI#77196-52602.

†Benedictine University

‡St. Joseph's University
In this paper, we discuss the probabilities of obtaining cycles of various lengths in randomly chosen permutations. (For instance, exactly 1/5 of the 8! possible eight-person Pollyanna permutations contain a 5-cycle; see Theorem 3, below.) In these terms, the Hatchet probability \( P_n \) is the probability that a randomly chosen permutation will have no 1-cycles. In \([3]\), Klingsberg and Panichella treat \( P_n \), the probability that \( \sigma \) will have no \( k \)-cycles. Here, we extend the discussion in \([3]\). We find the full distribution of the random variable \( X_n^k(\sigma) \), the number of \( k \)-cycles in the DCF of \( \sigma \) we calculate, for each \( 1 \leq k_1 < k_2 < \cdots < k_r \leq n \), the probability that \( \sigma \) contains no cycles of any of the lengths \( k_1 \) through \( k_r \) in its DCF; we use this probability to determine the joint distribution of the random variables \( \{X_n^{k_1}, \ldots, X_n^{k_r}\} \); and we obtain asymptotic expressions in each case.

2. The Principle of Inclusion-Exclusion. In order to make this paper more self-contained, we include a short account of the Principle of Inclusion-Exclusion (or PIE), which is an essential tool here. (This is the same account that appears in \([3]\).)

We state Proposition 1 without proof; it is a routine generalization of Theorem 1 in \([3]\).

**Proposition 1.** Let \( S \subseteq P \) be some subset of \( P \). Then

\[
N_\pi(S) = \sum_{S' \subseteq P} (-1)^{|S'|} N_\pi(S')
\]

where \( N_\pi(S) \) is the number of \( \pi \)-possessing \( \omega \)’s in \( S \).

We employ the PIE, taking \( S \) to denote the number of \( \pi \)-possessing \( \omega \)’s in \( S \).

Next, for each choice of parameters \( t_1, \ldots, t_r \), we can gather terms: since the summands in (2) depend only on the parameters \( t_1, \ldots, t_r \), we can write:

\[
N_\pi(S) = \sum_{S' \subseteq P} (-1)^{|S'|} N_\pi(S')
\]

(\( N_\pi(S) \) is the number of permutations with no fixed points.)

3. The probability of no cycles of the prescribed lengths.

**Definition.** For any choice \( 1 \leq k_1 < k_2 < \cdots < k_r \leq n \), let \( P_{k_1,k_2,\ldots,k_r} \) denote the probability that an element \( \sigma \) chosen uniformly at random from \( S_n \) contains no cycles of any of the lengths \( k_1, k_2, \ldots, k_r \).

Our first main result is a formula for \( P_{k_1,k_2,\ldots,k_r} \). We employ the PIE, taking \( S \) to be the set of all possible cycles of length \( \ell \), where \( \ell \in \{k_1, \ldots, k_r\} \).

As an example, \( P_{k_1} \) is the probability that \( \sigma \) contains no fixed points. Then \( P_{k_1} = \frac{n!}{(n-k_1)!} \left(1 - \frac{1}{n} \right) \)

Finally, \( P_{k_1,k_2,\ldots,k_r} \) is the probability that \( \sigma \) contains no cycles of lengths \( k_1, k_2, \ldots, k_r \), and we obtain asymptotic expressions in each case.

**Theorem 3.** For any choice \( 1 \leq k_1 < k_2 < \cdots < k_r \leq n \),

\[
P_{k_1,k_2,\ldots,k_r} = \sum_{t_1 \geq 0, t_2 \geq 0, \ldots, t_r \geq 0} \frac{(-1)^{t_1+\cdots+t_r}(n - (k_1 t_1 + \cdots + k_r t_r)!)}{(k_1 t_1)! \cdots (k_r t_r)!}
\]

Proof. Obviously, \( P_{k_1,k_2,\ldots,k_r} = N_\pi(\{0\})/n! \); and, by equation (1),

\[
N_\pi(\{0\}) = \sum_{S \subseteq P} (-1)^{|S|} N_\pi(S)
\]

Proposition 1 then allows us to restrict the sum above to subsets \( S \subseteq P \) such that all of the cycles in \( S \) are pairwise disjoint:

\[
N_\pi(\{0\}) = \sum_{S \subseteq P} (-1)^{|S|} N_\pi(S)
\]

and, if \( S \) has \( t_i \) cycles of length \( k_i \) for each \( 1 \leq i \leq r \), this becomes

\[
N_\pi(\{0\}) = \sum_{S \subseteq P} (-1)^{|S|} N_\pi(S)
\]

Now, since the summations in (2) depend only on the parameters \( t_1, \ldots, t_r \), we can gather terms:

\[
N_\pi(\{0\}) = \sum_{S \subseteq P} (-1)^{|S|} N_\pi(S)
\]

where \( \pi \) stands for the number of sets \( S \subseteq P \) with \( t_i \) cycles, \( 1 \leq i \leq r \), and with all cycles pairwise disjoint.

Next we compute \( \pi \). For each choice of parameters \( t_1, \ldots, t_r \), each subset \( S \subseteq P \) described in \( \pi \) can be uniquely constructed by doing each of the following:

**Step 1.** Choosing the elements of \([n]\) to be used in the cycles of \( S \). There are

\[
\binom{n}{k_1 t_1 + \cdots + k_r t_r}
\]

ways to do this.

**Step 2.** Dividing the elements chosen in Step 1 into \( r \) subsets of sizes \( (k_1 t_1, \ldots, k_r t_r) \) respectively. The elements of the \( i \)-th subset \( 1 \leq i \leq r \) will be included in some \( k_i \) cycle. There are

\[
\frac{(k_1 t_1 + \cdots + k_r t_r)!}{(k_1 t_1)! \cdots (k_r t_r)!}
\]

ways to do this, since this is an ordered choice.
Step 3. Partitioning each of the sets of size \( k_i \), chosen in Step 2 into \( t_i \) classes, each containing \( k_i \) elements. There are 
\[
\prod_{i=1}^{r} \frac{(k_i t_i)!}{(k_i)!^t_i t_i!}
\]
ways to do this, since each of these partitions is an unordered partition into classes of equal size.

Step 4. Arranging each subset chosen in Step 3 into a cycle. Since there are \((k_i - 1)!\) ways to do this for each \( k_i \)-element subset, there are in all 
\[
\prod_{i=1}^{r} \frac{(k_i - 1)!}{t_i!}
\]
possibilities for Step 4.

Multiplying all of these together and simplifying now gives the expression we need for \((*)\):
\[
(*) = \frac{n!}{(n - (k_1 t_1 + \cdots + k_r t_r))!} \prod_{i=1}^{r} \frac{1}{k_i! t_i!}.
\]

Substituting \((*)\) into (3) and simplifying yields
\[
N_n(\emptyset) = n! \left( \sum_{r_1, \ldots, r_r \geq 0, \sum r_i = n} \left( \prod_{i=1}^{r} \frac{(-1)^{r_i}}{t_i!} \right) \right),
\]
and dividing by \(n!\) then gives the result. \(\square\)

A consequence of this theorem is the asymptotic behavior of \(P_{n,k_1,\ldots,k_r}\):

**Corollary 4.** For any choice \(1 \leq k_1 < k_2 < \cdots < k_r\),
\[
\lim_{n \to \infty} P_{n,k_1,\ldots,k_r} = e^{- \left( \frac{k_1}{1} + \cdots + \frac{k_r}{r} \right)}.
\]

4. The full joint distribution. We next consider probabilities of obtaining positive numbers of cycles of various lengths. We continue to consider the experiment of choosing an element \(\sigma\) uniformly at random from \(S_n\).

**Definition 5.** For each \(1 \leq k \leq n\), let \(X_k^\sigma\) be the random variable
\[
X_k^\sigma(\sigma) := \text{the number of} \ k \text{-cycles in the DCF of} \ \sigma.
\]

Thus, in terms of these random variables,
\[
P_{n,k_1,\ldots,k_r} = \left( X_{k_1}^\sigma = 0 \right) \wedge \left( X_{k_2}^\sigma = 0 \right) \wedge \cdots \wedge \left( X_{k_r}^\sigma = 0 \right).
\]

We now consider the full distributions of these random variables, both singly and together.\(^1\)

**Theorem 6.** For any \(1 \leq k \leq n\) and any \(0 \leq m \leq \lfloor n/k \rfloor\),
\[
P[X_k^n = m] = \frac{1}{m! k^m} \sum_{t=0}^{\lfloor n/k \rfloor} \frac{(-1)^t}{t!}.
\]

(\(\text{Note that when} \ mk > n, \ \text{sum in} \ (4) \ \text{is empty, so that} \ (4) \ \text{gives the correct answer zero in this case.}\))

**Proof.** Each element \(\sigma \in S_n\) that contains exactly \(m\) \(k\)-cycles can be uniquely constructed by performing each of the following steps.

**Step 1.** Choosing \(m\) pairwise disjoint \(k\)-cycles for the DCF of \(\sigma\); and

**Step 2.** Choosing a permutation containing no \(k\)-cycles for the remaining \((n - mk)\) elements of \([n]\).

By a counting argument very similar to that in the proof of Theorem 1, the number of ways to carry out Step 1 is
\[
\binom{n}{mk} \cdot \frac{m!}{m! (k!^m)} \cdot \frac{(k-1)!^m}{(k-1)!^m} = \frac{n!}{mk! (n - mk)!}.
\]

The number of choices for performing Step 2 is \((n - mk)!P_{n - mk,\ldots,\ldots}\); and Theorem 2 of \([3]\) gives that
\[
(n - mk)!P_{n - mk,\ldots,\ldots} = \frac{n!}{mk! (n - mk)!} \sum_{t=0}^{\lfloor n/k \rfloor} \frac{(-1)^t}{t!}.
\]

Multiplying (5) by (6) and dividing by \(n!\) then gives the theorem. \(\square\)

Again, it is easy to find the asymptotic probability:

**Corollary 7.**
\[
\lim_{n \to \infty} P[X_k^n = m] = e^{-\lambda} \left( \frac{\lambda}{m!} \right)^m.
\]

Observe that this says that asymptotically, \(X_k^n\) has a Poisson distribution with mean \(\lambda = \frac{1}{k}\).

Our final two results deal with the full joint distribution of the random variables \(\{X_{k_1}^\sigma, \ldots, X_{k_r}^\sigma\}\). The proof of Theorem 5 combines elements of the proofs of Theorems 1 and 3.

**Theorem 8.** Fix \(1 \leq k_1 < \cdots < k_r\), and for any ordered choice \((m_1, \ldots, m_r)\) of nonnegative integers, let \(\zeta = k_1 m_1 + \cdots + k_r m_r\). Then for any \(n \geq \zeta\), we have that
\[
P[(X_{k_1}^\sigma = m_1) \wedge (X_{k_2}^\sigma = m_2) \wedge \cdots \wedge (X_{k_r}^\sigma = m_r)] = \frac{1}{m_1! m_2! \cdots m_r!} \sum_{r_1, \ldots, r_r \geq 0, \sum r_i = \zeta} \left( \prod_{i=1}^{r} \frac{(-1)^{r_i}}{t_i!} \right)
\]

\(\text{Proof.}\) If \(\sigma \in S_n\) contains exactly \(m_i\) cycles of length \(k_i\), \(1 \leq i \leq r\), then \(\sigma\) can be uniquely constructed by doing each of the following.

**Step 1.** Choosing \(\zeta\) elements from \([n]\) out of which to construct \(m_i\) cycles of length \(k_i\), \(1 \leq i \leq r\); this can be done in \(\binom{n}{\zeta}\) ways.

\(\square\)
Step 2. Dividing all elements chosen in Step 1 into \( r \) subsets of sizes \((k_1m_1, \ldots, k_rm_r)\) respectively. The elements of the \( i \)-th subset \((1 \leq i \leq r)\) will be included in some \( k_i \) cycle. There are

\[
\frac{\zeta!}{(k_1m_1)! \cdots (k_rm_r)!}
\]

ways to do this, since this is an ordered choice.

Step 3. Partitioning each of the sets of size \( km_i \) chosen in Step 2 into \( m_i \) classes, each containing \( k_i \) elements. There are

\[
\prod_{i=1}^{r} \left( \frac{(km_i)!}{(k_i)!^{m_i} \cdot m_i!} \right)
\]

ways to do this, since each of these partitions is an unordered partition into classes of equal size.

Step 4. Arranging each subset chosen in Step 3 into a cycle. Since there are \((k_i-1)!\) ways to do this for each \( k_i \)-element subset, there are in all

\[
\prod_{i=1}^{r} ((k_i - 1)!)^{m_i}
\]

possibilities for Step 4.

Step 5. Choosing for the remaining \((n-\zeta)\) elements of \([n]\) a permutation that has no cycle of any of the lengths \( k_1 \) through \( k_r \). By Theorem 1, this can be done in exactly

\[
(n-\zeta)! \left( \sum_{k_1t_1 + \cdots + k_rt_r \leq n-\zeta} \left( \prod_{i=1}^{r} \frac{(-1)^{t_i}}{t_i!} \right) \right)
\]

ways.

Multiplying all of these together, simplifying, and dividing by \( n! \) now gives the theorem.

Taking the limit as \( n \to \infty \) of (7) simply removes the condition

\[
k_1t_1 + \cdots + k_rt_r \leq n - \zeta
\]

from the sum there. Then, a routine series manipulation gives Corollary 6, below. It says, that asymptotically, the random variables \( \{X_{k_1}^n, \ldots, X_{k_r}^n\} \) are independent (and Poisson).

Corollary 9. With \( 1 \leq k_1 < \cdots < k_r \) and \((m_1, \ldots, m_r)\) as in Theorem 5, we have

\[
\lim_{n \to \infty} P[(X_{k_1}^n = m_1) \land (X_{k_2}^n = m_2) \land \cdots \land (X_{k_r}^n = m_r)] = \prod_{i=1}^{r} \frac{e^{-\frac{m_i}{k_i}}}{m_i!^{k_i/m_i}}
\]

REFERENCES


Wendy L. Corp, Department of Mathematics, University of Kentucky, Lexington KY 40506, Email: wcorp@ms.uky.edu

Theresa L. Friedman, Department of Mathematics, Willamette University, 900 State St., Salem OR 97301, Email: friedmat@willamette.edu

Paul Klingsberg, Department of Mathematics and Computer Science, St. Joseph's University, 5600 City Ave., Philadelphia PA 19131, Email: pklingsb@sju.edu

In the 2000-2001 academic year, Wendy Corp was a senior majoring in mathematics at Benedictine University. She graduated in May, 2001 with a B.S. in mathematics, and in September, 2001, she began graduate studies in mathematics at the University of Kentucky. Ms. Corp is a member of both IIME and KME. At Mathfest 2000, she received an Award for Outstanding Presentation for her presentation of the results reported here.

Theresa Friedman completed her Ph.D. in mathematics from Lehigh University in 1997. The work on this paper was completed while she was on the faculty of Benedictine University. She is currently on the faculty of Willamette University.

Paul Klingsberg earned his Ph.D. in mathematics from the University of Pennsylvania in 1977. He has been on the faculty of St. Joseph's University since 1981.
If you’re a student preparing to become a teacher, the best thing you can do for your professional development is to join NCTM.

Membership opens the door to top-notch educational resources, award-winning journals, and dynamic conferences. Become a student member today and take advantage of our special student rate of $34. As a student, you are also eligible for special benefits—FREE admission to NCTM Regional Conferences and reduced rates for the Annual Meeting.

As a future teacher, you need the most effective math education tools available. Membership in NCTM will ensure that you have all you’ll ever need.

Join today and discover the possibilities!

For more information or to join, visit www.nctm.org/membership or call (800) 235-7566.

AN INFINITE-DIMENSIONAL LUCAS MATRIX

THOMAS KOSHY

In 1966, D. M. Bloom proposed the following problem [1]: Determine

\[ \sum_{i+j+k=n} F_i F_j F_k \]

where \( F_n \) denotes the \( n \)-th Fibonacci number, defined recursively as follows:

\[
F_1 = F_2 = 1 \\
F_n = F_{n-1} + F_{n-2}, n \geq 3
\]

This definition can in fact be extended by defining \( F_0 = 0 \) and \( F_{-1} = 1 \). In the following year, C. Libis provided an interesting solution to the problem [2].

Fibonacci numbers and Lucas numbers \( L_n \), named after the French mathematician François-Édouard-Anatole Lucas (1842-1891), share many similar properties. They are defined by

\[
L_1 = 1, L_2 = 3 \\
L_n = L_{n-1} + L_{n-2}, n \geq 3
\]

This definition also can be extended by letting \( L_0 = 2 \) and \( L_{-1} = -1 \). A study of Lucas numbers, similar to Bloom’s, yields some interesting and rewarding dividends.

To this end, consider the infinite dimensional matrix \( K = (k_{ij}) \):

\[
K = \begin{bmatrix}
K_{0,n} \\
K_{1,n} \\
\vdots \\
K_{n,n}
\end{bmatrix}
\]

where each element \( k_{ij} \) is defined recursively as follows for \( i, j \geq 0 \).

\[
\begin{align*}
(1) \quad k_{0,j} & = 0 \\
(2) \quad k_{1,1} & = 1 \\
(3) \quad k_{j,j-1} & = 2, \quad j \geq 1 \\
(4) \quad k_{i,j} & = 0, \quad j < i - 1 \\
(5) \quad k_{i,j} & = k_{i,j-2} + k_{i,j-1} + k_{i-1,j-1}, \quad i \geq 1, j \geq 2
\end{align*}
\]

Condition (1) implies that row 0 consists of zeros; conditions (2) and (3) imply the first two elements in row 1 are 2 and 1; by condition (3), the diagonal below the main diagonal consists of twos; and by condition (4), every element below this diagonal is zero. Condition (5) can now be employed to compute the remaining elements \( k_{ij} \) of \( K \): add the two previous elements \( k_{i,j-2} \) and \( k_{i,j-1} \) in row \( i \), and then add this sum to the element \( k_{i-1,j-1} \) just above \( k_{i,j} \):

\[
\begin{align*}
&k_{i-1,j-1} \\
&k_{i,j-2} + k_{i,j-1} = k_{i,j}
\end{align*}
\]
Thus

\[
\begin{array}{cccccccc}
\mathbf{K} = & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
2 & 0 & 2 & 3 & 8 & 15 & 30 & 56 \\
3 & 0 & 0 & 2 & 5 & 15 & 35 & 80 \\
4 & 0 & 0 & 0 & 2 & 7 & 24 & 66 \\
5 & 0 & 0 & 0 & 0 & 2 & 9 & 35 \\
6 & 0 & 0 & 0 & 0 & 0 & 2 & 11 \\
\end{array}
\]

Lucas Numbers

Using the recursive formula, we have:

\[
k_{1,n} = k_{1,n-2} + k_{1,n-1} + k_{0,n-1}
\]

Since \(k_{1,0} = 2\) and \(k_{1,1} = 1\), it follows that \(k_{1,n} = L_n\), so row 1 consists entirely of Lucas numbers.

Here is an interesting observation:

\[
k_{2,7} = 104 = 1 \cdot 18 + 1 \cdot 11 + 2 \cdot 7 + 3 \cdot 4 + 5 \cdot 3 + 8 \cdot 1 + 13 \cdot 2
\]

\[
= \sum_{j=1}^{7} F_j k_{1,7-j} = \sum_{j,k \in \mathbb{N}} F_j L_k
\]

More generally, we have the following result, which we establish using strong induction.

**Theorem 1.** With \(k_{i,j}\) defined as above,

\[
k_{2,n} = \sum_{j,k \in \mathbb{N}} F_j L_k
\]

**Proof.** When \(n = 0\), each side equals zero, so the result is true.

Now assume that it is true for every nonnegative integer less than or equal to \(m\):

\[
k_{2,m} = \sum_{j,k \in \mathbb{N}} F_j L_k
\]

Then

\[
\sum_{j,k \in \mathbb{N}} F_j L_k = \sum_{j=0}^{m+1} F_j L_{m+1-j} = \sum_{j=0}^{m} F_j (L_{m-j} + L_{m-j-1}) + F_{m+1} L_0
\]

Since \(k_{1,s} = L_s\), formula (1) can be written as

\[
k_{2,n} = \sum_{j,k \in \mathbb{N}} F_j k_{1,t}
\]

In words, every element \(k_{2,n}\) can be obtained by multiplying the elements \(k_{1,n-1}, k_{1,n-2}, \ldots, k_{1,0}\) in the previous row with weights \(F_1, F_2, \ldots, F_n\) respectively, and then adding up the products, as we observed earlier.

As in Theorem 1, it can be proved that

\[
k_{3,n} = \sum_{i=0}^{n} F_i k_{2,n-i} = \sum_{i,j,k \in \mathbb{N}} F_i F_j L_k
\]

**Formula (3)**

For example,

\[
k_{3,5} = F_0 k_{2,5} + F_1 k_{2,4} + F_2 k_{2,3} + F_3 k_{2,2} + F_4 k_{2,1} + F_5 k_{2,0}
\]

\[
= 0 \cdot 30 + 1 \cdot 15 + 1 \cdot 8 + 2 \cdot 3 + 3 \cdot 2 + 5 \cdot 0
\]

\[
= 35
\]

Formulas (1) and (3) are in fact special cases of the following result, which also can be established using strong induction.

**Theorem 2.** With \(k_{i,j}\) defined as above,

\[
k_{m,n} = \sum_{i=0}^{n} F_i k_{m-1,n-i}, m \geq 2
\]

**Proof.** By Theorem 1, the result is true when \(m = 2\), so we assume that \(m \geq 3\). Keeping \(m\) fixed, we shall prove that formula (4) works for all \(n \geq 0\). Since \(k_{m,0} = 0 = \sum_{i=0}^{m} F_i k_{m-1,i}\), the result is true when \(n = 0\). It is also true when \(n = 1\).

Now assume the result is true for all nonnegative integers less than or equal to an arbitrary integer \(t\), where \(t \geq 2\):

\[
k_{m,t} = \sum_{i=0}^{t} F_i k_{m-1,t-i}
\]
Then:

\[
\sum_{i=0}^{t+1} F_i k_{m-1,i+1} - i = \sum_{i=0}^{t+1} F_i k_{m-1,i+1} - i + F_i k_{m-1,1} + F_i k_{m-1,0}
\]

\[
= \sum_{i=0}^{t} F_i k_{m-1,i+1} - i + \sum_{i=0}^{t} F_i k_{m-1,i+1} + F_i k_{m-1,1} + F_i k_{m-1,0}
\]

\[
= \sum_{i=0}^{t} F_i k_{m-1,i+1} - i + \sum_{i=0}^{t} F_i k_{m-1,i+1} + F_i k_{m-1,1} + F_i k_{m-1,0}
\]

\[
= \sum_{i=0}^{t} (F_i k_{m-1,i+1} - i) + R
\]

where \( R = F_1 k_{m-1,1} + F_1 k_{m-1,0} - F_1 k_{m-2,0} \)

If \( m = 3 \), then:

\[
R = F_1 k_{m-1,1} + F_1 k_{m-1,0} - F_1 k_{m-2,0}
\]

\[
= F_1 k_{m-1,1} + F_1 k_{m-1,0} - F_1 k_{m-2,0}
\]

\[
= 2F_t + 0 - 2F_t = 0
\]

On the other hand, if \( m > 3 \), then \( R = 0 \). Thus, in both cases, \( R = 0 \).

So

\[
\sum_{i=0}^{t+1} F_i k_{m-1,i+1} - i = k_{m,t+1} + k_{m,t} + k_{m-1,t} + 0 = k_{m,t+1}
\]

Therefore, by strong induction, formula (4) is true for all \( m \geq 3 \) and hence true for all \( m \geq 2 \).

For example,

\[
k_{4,5} = \sum_{i=0}^{5} F_i k_{3,5-i} = \sum_{i=1}^{4} F_i k_{3,5-i} = F_1 k_{3,4} + F_2 k_{3,3} + F_3 k_{3,2} + F_4 k_{3,1}
\]

\[
= 15 + 5 + 4 + 0 = 24
\]

Explicit Formulas for \( k_{2,n} \) and \( k_{3,n} \). Row 2 of matrix \( K \) contains an intriguing pattern:

\[
\begin{align*}
  k_{2,0} &= 0 = 1 \cdot F_0 \\
  k_{2,1} &= 2 = 2 \cdot F_1 \\
  k_{2,2} &= 3 = 3 \cdot F_2 \\
  k_{2,3} &= 8 = 4 \cdot F_3 \\
  k_{2,4} &= 15 = 5 \cdot F_4 \\
\end{align*}
\]

where \( F_n \) is the \( n \)th Fibonacci number. So we conjecture that \( k_{2,n} = (n + 1)F_n \). The next theorem in fact confirms it using strong induction.

**Theorem 3.** With \( k_{i,j} \) defined as above,

\[
k_{2,n} = (n + 1)F_n
\]

**Proof.** Since \( k_{2,0} = 0 = (0 + 1)F_0 \), the result is true for \( n = 0 \). Now assume it is true for all nonnegative integers \( \leq t \), where \( t \) is greater than or equal to 0. Then:

\[
\begin{align*}
  (t + 2)F_{t+1} - (t + 1)F_t - F_{t+1} &= 0 \\
  &= tF_{t+1} + (t + 1)F_t + 2F_{t-1}
\end{align*}
\]

But \( F_t + 2F_{t-1} = F_{t+1} + F_{t-1} = L_t \). Therefore,

\[
\begin{align*}
  (t + 2)F_{t+1} &= tF_{t+1} + (t + 1)F_t + L_t \\
  &= k_{2,t+1} + k_{2,t} + k_{1,t} + a_{2,t+1}
\end{align*}
\]

Thus, by strong induction, formula (5) is true for all \( n \geq 0 \).

Formula (5) can also be established by assuming that \( k_{3,n} \) is of the form \((an + b)F_n + (cn + d)F_{n-1}\), as in [2].

Again, as in [2], \( k_{3,n} \) must be of the form \((an^2 + bn + c)F_n + (dn^2 + en + f)F_{n-1}\).

Using the initial values of \( k_{3,0} \) through \( k_{3,5} \), it can be seen that \( a = 1/10 = b = c = -1/5 = -d, e = 2/5, \) and \( f = 0 \). This yields

\[
k_{3,n} = \frac{(n^2 + 2n - 2)F_n + 2n(n + 2)F_{n-1}}{10}
\]

Since \( F_n + 2F_{n-1} = L_n \), this can be rewritten as

\[
k_{3,n} = \frac{(n + 2)(nL_n - F_n)}{10}
\]

For example, \( k_{3,7} = 9(7L_7 - F_7)/10 = 9(7 \cdot 29 - 13)/10 = 171 \) as expected.

As a byproduct, it follows from (6) that \((n + 2)(nL_n - F_n) \equiv 0 \pmod{10}\); thus if \( n + 2 \) and 10 are relatively prime, then \( nL_n \equiv F_n \pmod{10} \). For example, \( 7L_7 \equiv 3 \equiv F_7 \pmod{10} \).

More generally, suppose we construct a new matrix \( G \) which also satisfies conditions (1), (4) and (5), and two new conditions:

\[
\begin{align*}
  (2') \quad G_{1,1} &= a \\
  (3') \quad G_{1,2} &= b
\end{align*}
\]
where \( a \) and \( b \) are arbitrary integers, and \( G_{1,0} = b - a \). Then \( G \) is

\[
\begin{array}{cccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & \ldots \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & b - a & a & b + a & a + 2b & 2a + 3b & 3a + 5b & \leftarrow \text{GFNs} \\
2 & 0 & b - a & 3b - a & 5b & 10b & 2a + 3b & \ldots \\
3 & 0 & 0 & b - a & 2b - a & 6b - 3a & 13b - 4a & 29b - 7a \\
\vdots & & & & & & & \\
\end{array}
\]

Row 1 of \( G \) consists of the generalized Fibonacci numbers (GFN’s) \( G_n \); when \( a = 1 = b \), \( G_n = F_n \); and when \( a = 1 \) and \( b = 3 \), \( G_n = \phi_n \).

Formula (4) can be extended to \( G \), as the next theorem shows. Its proof follows along the same lines as in Theorem 2, so we skip it.

**Theorem 4.** With \( G_{m,n} \) defined as above,

\[
G_{m,n} = \sum_{i=0}^{n-1} F_i G_{m-1,n-i}, \quad m \geq 2
\]

For example,

\[
G_{3,5} = \sum_{i=0}^{4} F_i G_{3,5-i} = F_0 G_{3,5} + F_1 G_{3,4} + F_2 G_{3,3} + F_3 G_{3,2} + F_4 G_{3,1} = 5b + (3b - a) + 2b + 3(b - a) = 13b - 4a
\]

In particular, when \( m = 2 \) and \( m = 3 \), formula (7) yields

\[
G_{2,n} = \sum_{i=0}^{n} F_i G_{1,n-i} = \sum_{i=0}^{n} F_i G_{n-i}
\]

and

\[
G_{3,n} = \sum_{i=0}^{n} F_i G_{2,n-i} = \sum_{i=0}^{n} F_i F_j G_k
\]

**Acknowledgement.** The author wishes to thank the referee for his/her helpful suggestions for the improvement of the original version of the article.

**REFERENCES**


Thomas Koshy, Department of Mathematics, Framingham State College, Framingham, MA 01701-9101. E-mail: tkoshy@fsc.mass.edu

Thomas Koshy received his Ph.D. from Boston University and has been on the faculty of Framingham State College since 1970.

---

**THE PROBABILITY OF RANDOMLY GENERATING A FINITE GROUP**

KIMBERLY L. PATTI*

1. **Introduction.** This article considers the problem, given a finite group \( G \) with \( n \) generators, what is the probability that \( n \) randomly chosen elements will generate \( G \). From Deborah L. Massari we know that the probability that a randomly chosen element from a cyclic group is a generator of this group depends only on the set of prime divisors of the order of the group, rather than the size of the group [3]. In this article we investigate this problem for some specific finite cyclic and non-cyclic groups. Examples for these specific groups are also provided.

We will consider the following groups:

1. Cyclic groups of order \( p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \), where the \( p_i \) are prime and the \( e_i \) are positive integers
2. \( \mathbb{Z}_p \oplus \mathbb{Z}_q \oplus \cdots \oplus \mathbb{Z}_m \), where \( p \) is prime
3. \( D_n \), the dihedral groups.

Throughout this paper, we consider the event that \( n \) randomly chosen elements in an \( n \) generated group generate the group. We refer to this as event \( A \), and we investigate the probability of \( A \).

2. **Cyclic Groups.** Let \( G \) be a cyclic group such that \( G = \langle a \rangle \) and \( |G| = n \), where \( n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \). \( G = \langle a^p \rangle \) if and only if \( \gcd (j, n) = 1 \) (see, for example, [2, Theorem 4.2]). Generators of \( G \) are elements of order \( n \), so we need to find all such elements. The number of elements of order \( n \) in a cyclic group is determined by the Euler phi function, \( \phi \), where \( \phi (n) \) equals the number of positive integers less than \( n \) and relatively prime to \( n \) (see, for example, [1, p. 7]). Thus,

\[
\phi (p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = p_1^{e_1 - 1} (1 - \frac{1}{p_1}) p_2^{e_2 - 1} (1 - \frac{1}{p_2}) \cdots p_k^{e_k - 1} (1 - \frac{1}{p_k}).
\]

So

\[
P(A) = \frac{p_1^{e_1 - 1} (1 - \frac{1}{p_1}) p_2^{e_2 - 1} (1 - \frac{1}{p_2}) \cdots p_k^{e_k - 1} (1 - \frac{1}{p_k})}{p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}}
\]

Notice that this formula does not depend on the powers of \( p_i \). So, for example, for \( G = \mathbb{Z}_{270} = \mathbb{Z}_{2^2 \cdot 3^3 \cdot 5} \) and \( H = \mathbb{Z}_{2469} = \mathbb{Z}_{2^2 \cdot 3^2 \cdot 7 \cdot 11} \), \( P(A) \) is the same.

**Example:** Let \( G = \mathbb{Z}_6 \oplus \mathbb{Z}_{14} \oplus \mathbb{Z}_{13} \oplus \mathbb{Z}_{33} \oplus \mathbb{Z}_{59} \). For this group, \( P(A) \) would be incredibly difficult to calculate by simple observation. We can use the previous formula, however, to simplify the process. Since 6, 35, 143, 323, and 667 are relatively prime, we have that \( G \) is isomorphic to the cyclic group \( \mathbb{Z}_{63493230} \). Also, we know that \( |G| = (6)(35)(143)(323)(667) = (2)(3)(5)(7)(11)(13)(17)(19)(23)(29) \). So, by formula (1), \( P(A) \) is given by

\[
(1 - \frac{1}{6})(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{2})(1 - \frac{1}{7})(1 - \frac{1}{11})(1 - \frac{1}{13})(1 - \frac{1}{17})(1 - \frac{1}{19})(1 - \frac{1}{23})(1 - \frac{1}{29}).
\]

*Saint Louis University*
Thus $P(A) \approx .1579$.

3. The Group $Z_p \oplus Z_p \oplus \cdots \oplus Z_p$, where $p$ is prime. We first consider the group $Z_p \oplus Z_p$. This group can be generated by two elements. For $a, b, c, d \in Z_p$ \((a, b, c, d)\) generates $Z_p \oplus Z_p$ if and only if there exist $r_1, r_2, r_3, r_4$ in $Z$ such that $r_1(a, b) + r_2(c, d) = (1, 0)$ and $r_3(a, b) + r_4(c, d) = (0, 1)$. Thus, we need to solve the system

$$
\begin{align*}
    a &= r_1 + r_3, \\
    b &= r_3, \\
    c &= r_1, \\
    d &= r_2 + r_4.
\end{align*}
$$

In order to solve these systems, we must take the inverse of $A$, which exists if and only the columns of $A$ are independent. The first column, $(a, b, c, d)$, can be anything except the zero vector. Thus, there are $p^2 - 1$ choices for the next column. The next column must be chosen so that it is not a multiple of $(a, b)$. Since we are in $Z_p \oplus Z_p$, there are $p$ such ordered pairs. Thus, given $(a, b)$, there are $p^2 - p$ choices for the column $(c, d)$. Therefore, the number of choices for the pair $(a, b, c, d)$ is $((p^2 - 1)(p^2 - p))/2$. We divide by 2 since order does not matter. So there are $((p^2 - 1)(p^2 - p))/2$ ways to choose $(a, b)$ and $(c, d)$ such that $(a, b, c, d)$ generates $Z_p \oplus Z_p$. Thus,

$$
P(A) = \left(\frac{p^2 - 1}{2}\right) \left(\frac{p^2 - 1}{2}\right) = \frac{p^2 - 1}{p}.
$$

It is interesting to notice that this formula is the same as the one for $Z_p$.

Similarly, we can find $P(A)$ for $Z_p \oplus Z_p \oplus \cdots \oplus Z_p$, where the direct product of $Z_p$ is taken $n$ times. Notice that we can set up a system of equations in matrix form. As before, we want the columns of our matrix to be independent, which happens if and only if our matrix has rank $n$. In the $i^{th}$ column, there are $p^n - p^{i-1}$ ways to choose an $n$-tuple so that the $i^{th}$ column is linearly independent of the first $i - 1$ columns. Thus, there are

$$
\frac{1}{n!} \prod_{i=0}^{n-1} (p^n - p^i)
$$

ways to choose our $n$-tuples so that they generate the group. Therefore,

$$
P(A) = \left(\frac{p^n}{n!}\right) \prod_{i=0}^{n-1} (p^n - p^i).
$$

**Example:** Let $G = Z_7 \oplus Z_7 \oplus Z_7 \oplus Z_7 \oplus Z_7$. Then $|G| = 7^5 = 16807$. Using formula (3), we see that

$$
P(A) = \left(\frac{7^5}{5!}\right) \prod_{i=0}^{4} (7^5 - 7^i) = \frac{7^5}{5!} (7^5 - 7^4)(7^5 - 7^3)(7^5 - 7^2)(7^5 - 7^1) \approx 8373.
$$

4. $D_n$, the Dihedral Groups, where $n$ is a positive integer. Let $D_n$ denote the group of symmetries of a regular $n$-gon, where $n = p^i_1 p^2_3 \cdots p^k_6$. The dihedral groups are composed of a subgroup of rotations and a subset of reflections. Although

the dihedral groups are not cyclic, they can be generated by two elements. There are two possible combinations of reflections and rotations that generate $D_n$. In the first, we need one reflection and one rotation of order $n$. Another possibility occurs when choosing two reflections. The reflections must be chosen so that together they produce a rotation of order $n$. Thus, we can generate the dihedral groups by choosing one reflection and one rotation, or by choosing two reflections. Let $B$ be the event of randomly choosing a reflection, and let $C$ be the event of randomly choosing a rotation of order $n$. Let $D$ be the event of randomly choosing a second reflection that, together with the first, will generate all of $D_n$. Then $P(B \cap C)$ gives us the probability of our first possible way to generate $D_n$, and $P(B \cap D)$ will give us the probability of our second possible way to generate $D_n$. Thus, $P(A) = P(B \cap C) + P(B \cap D)$.

Since there are $n$ reflections and $\phi(n)$ rotations of order $n$ we have

$$
P(B \cap C) = \left(\frac{2^n}{2}\right) \left(\frac{n}{\phi(n)}\right) = \frac{(2(2n - 2))!n!n!}{(2^n)!} = \frac{\phi(n)}{2n - 1}.
$$

Now we need to find $P(B \cap D) = P(B)P(D|B)$. The elements in $D_n$ can be denoted by \((a, b, c, d)\), where $a$ is a rotation of order $n$, $b$ is a reflection, and $bd = a^{-1}b$ for $1 \leq j \leq n - 1$. Thus, $P(B) = 1/2$. If event $B$ occurs, we can denote the selected reflection by $b$. If the second element we choose is a reflection, we can denote it by $a'b$. To find $P(D | B)$, we need to find the probability that these two reflections produce a rotation of order $n$. Multiplying our two reflections together we have $ba'b = a'b2^j$. Thus, we need to know when $a^2$ is a rotation of order $n$. This occurs when $j$ is relatively prime to $n$. Thus, we can once again use the Euler phi function. Notice that we can again set up a system such that event $B$ has already occurred, so there are only $2n - 1$ elements to choose from. So

$$
P(B \cap D) = \frac{1}{2} \frac{\phi(n)}{2n - 1} = \frac{p_n(1 - \frac{1}{p_1})p_{p_1}(1 - \frac{1}{p_2})\cdots p_{p_k}(1 - \frac{1}{p_n})}{2(2n - 1)}.
$$

Now $P(A) = P((B \cap C) \cup (B \cap D)) = P(B \cap C) + P(B \cap D)$ since $P(B \cap C \cap D) = 0$. Thus,

$$
P(A) = P(B \cap C) + P(B \cap D) = \frac{3p_n(1 - \frac{1}{p_1})p_{p_1}(1 - \frac{1}{p_2})\cdots p_{p_k}(1 - \frac{1}{p_n})}{2(2n - 1)}.
$$

5. A Fun Example. Let $G = Z_9$ and let $H = Z_{16983563041}$. One might assume that the probability of randomly choosing a generator for $G$ would be greater than the probability of randomly choosing a generator for $H$ since $H$ is so much larger than $G$. The results, however, are surprising. Notice that $|G| = 6 = (2)(3)$ and $|H| = 16983563041 = 10^9$. Using formula (1) we obtain the following probabilities:

$$
P_G(A) = (1 - \frac{1}{2})(1 - \frac{1}{3}) = \frac{1}{6} \approx .1666, \\
P_H(A) = (1 - \frac{1}{2})(1 - \frac{1}{3}) = \frac{1}{2} = .5000.
$$

Thus, the probability of randomly choosing a generator in $H$ is actually much greater than the probability of randomly choosing a generator in $G$. Notice also that for any given $c < 1$ there exists a group such that $P(A) > c$ since $P(A) = 1 - 1/p$ for $G$ a cyclic group of prime order $p$. Using the previous example, we can find a group $K$ where $P(A)$ is greater than that in $H$ by choosing a prime larger than 19. So for $K = Z_{23}$, $P(A) > .947$. This method can be used for any of the prime numbers, with

**Randomly Generating a Finite Group**

315
the limit of $P(A)$ approaching 1. So for any cyclic group $G$, there exists a cyclic group $H$ such that the probability of randomly choosing a generator in $H$ is greater than the probability of randomly choosing a generator in $G$.

6. Acknowledgements. I would like to thank Dr. Russell Blyth and Dr. Greg Marks for reading this paper and providing helpful suggestions. I would also like to give a very special thanks to Dr. Julianne Rainbolt for giving me the opportunity to participate in undergraduate research and providing me with guidance and advice throughout the development of my research.

REFERENCES


9346 Southtowne Farms Dr., St. Louis, MO 63123-7048, pattikl@slu.edu

Kimberly L. Patti is an undergraduate at Saint Louis University. She began this paper in her junior year and finished it as an independent undergraduate research project. Kim expects to receive her B.S. in Mathematics in May 2002 and afterward attend graduate school to pursue a Ph.D. in Mathematics.

The Richard V. Andree Awards. The Richard V. Andree Awards are given annually to the authors of the papers, written by undergraduate students, that have been judged by the officers and councilors of Pi Mu Epsilon to be the best that have appeared in the Pi Mu Epsilon Journal in the past year.

Until his death in 1987, Richard V. Andree was Professor Emeritus of Mathematics at the University of Oklahoma. He had served Pi Mu Epsilon for many years and in a variety of capacities: as President, as Secretary-Treasurer, and as Editor of this Journal.

The awards for papers appearing in 2001 are announced on the next page. The officers and councilors of the Society congratulate the winners on their achievements and wish them well for their futures.

Emilia Huerta-Sanchez, Aida Navarro-Lopez, David Uminsky
"Iteration of an Even-Odd Splitting Map",

John Griesmer,
"Results Involving Continuity of the Derivative",
The American Mathematical Society was founded in 1888 to further mathematical research and scholarship. The Society currently has approximately 30,000 members throughout the United States and around the world. It fulfills its mission through programs that promote mathematical research, increase the awareness of the value of mathematics to society, and foster excellence in mathematics education.

The AMS invites members of Pi Mu Epsilon to take advantage of the special dues rate of $34 for student members. See www.ams.org/membership for details.

Visit the AMS Web site at www.ams.org/employment/undergrad.html to see the many resources available for undergraduates in mathematics.

Abstract. This article presents a simple two-person card game and the counter-intuitive conclusion to the question "Do you want to deal?".

1. Introduction. The dealer seems to have the advantage in many popular card games. Did you ever think about why you are not allowed to deal blackjack in the casinos of Las Vegas or Monte Carlo? In this article we describe a very simple two-person card game where the answer to the question, "Do you want to deal?", is not immediately apparent. The analysis of this game, which involves elementary aspects of combinatorics, probability, decision theory, infinite series, and game theory, provides some surprising results and instructive lessons concerning competitive strategies.

2. Description of the game. The dealer (a man) deals one card, from an ordinary, 52-card deck, to his opponent (a woman) and then one to himself. The object of the game is to end up with the higher card, where an Ace is considered low so that a King is the highest possible card. Each player looks at his/her card. First, if either player is dealt a King, that player must reveal it immediately. Next, the opponent has the option of trading her card with the dealer's, provided that neither card is a King.

If she decides to trade, both players look at their new cards as the trade is made. Then, the dealer has the option of trading his card with the top card (unseen to him) from the remaining deck. Finally, both players reveal their cards, and the one with the higher card is declared the winner. In the event of a tie, the game is replayed until one player wins.

The dealer seems to hold two advantages in this game:

- If the opponent elects to trade, the dealer instantly knows (since he will have seen both cards) whether he is a sure winner (and need not trade with the deck) or a potential loser (and therefore must trade with the deck).
- The dealer enjoys the possibility, which the opponent does not, of trading and receiving a King. The opponent cannot trade for a King because if the dealer has a King, he reveals it immediately and precludes the opponent's trading with him. It is possible, however, for the top card of the remaining deck to be a King, for which the dealer could trade.

The answer to the title question, "Do you want to deal?", would seem to be a resounding "Yes!"

3. Naive strategies. What strategy should each player adopt, i.e., when should one trade or keep one's card? One reasonable (but naive) approach might be for each player to trade only when the probability of bettering his/her card is greater than or equal to that of worsening it. Since the opponent has no chance of trading for a King (as mentioned above), her naive strategy is to trade with a Six or below, to stick with a Seven or above. To see this, note that if she has a Six, there are 24 cards (4 for each of the Seven through Queen) that would better hers and only 20 (4 for each of the Ace through Five) that would worsen it; with a Seven there are 20 cards that would better hers and 24 that would worsen it.

*California Polytechnic State University
†Dickinson College
The dealer, on the other hand, has the built-in advantage, for if he reveals a King or if the opponent trades or reveals a King, the dealer instantly knows whether or not he holds a winning card. If the dealer receives from the opponent a better card than he gave up, he should certainly not trade, for he is a sure winner. If he receives a worse card than the one he gave up or if the opponent reveals a King, he should certainly trade, for he is otherwise a sure loser. If he receives the same card or if the opponent does not trade (and does not reveal a King), the dealer’s naive strategy is still different from that of the opponent, for the dealer has the possibility of trading for a King from the deck. The dealer’s naive strategy is to trade with a Seven or below, to stick with an Eight or above. To see this, note that if he has a Seven, there are 24 cards (4 for each of the Eight through King) that would better his and also 24 (4 for each of the Ace through Six) that would worsen it; with an Eight there are only 20 cards (4 for each of the Nine through King) that would better his and 28 (4 for each of the Ace through Seven) that would worsen it.

Thus, the opponent’s naive strategy is to trade with a Six and below, stick with a Seven and above. For the dealer, the naive strategy is to trade with a Seven and below, stick with an Eight and above, unless he has an obvious choice determined by the opponent’s trading or revealing a King.

4. Analysis of naive strategies. To determine the probabilities of each player’s winning the game using these naive strategies, we first calculate the probabilities conditional on the pair of cards that is dealt. For example, if the dealer is dealt a Four and the dealer a Seven, the opponent (not knowing that she had the higher card) would trade, and the dealer (seeing that he received a higher card than he gave up) would stick, thus winning the game. Therefore, the conditional probabilities of winning the game given this particular deal are 0 for the opponent and 1 for the dealer.

As another example, suppose that the opponent is dealt a Five and the dealer an Eight. Then the opponent would trade (receiving the Eight), and the dealer (having received a worse card than he gave up) would trade with the remaining deck. The dealer would then win only if the top card from the remaining deck is a Nine or above; since there are 20 such cards (4 for each of the Nine through King) and 50 cards remaining in the deck (since a Five and an Eight were already dealt), this probability is 20/50. The opponent would win if the top card from the remaining deck is a Seven or below; since there are 27 such cards (4 for each of the Nine through King and 50 cards remaining in the deck (since a Five and an Eight were already dealt), this probability is 20/50. The probability of a tie is then 0 (corresponding to the top card from the remaining deck being one of the 3 remaining Eights).

For a third example, suppose that the opponent is dealt a Jack and the dealer a Seven. The opponent would keep her Jack, and the dealer would trade his Seven. The dealer would win if the top card from the remaining deck is a Queen or a King; there are 8 such cards, so the probability is 8/50. The opponent would win if the top card is below a Jack; there are 39 such cards (4 for each of the Ace through Ten, except only 3 for the Seven), so the probability is 39/50. The players would tie if the top card is one of the 3 remaining Jacks, which has probability 3/50.

Table 4.1 contains the conditional probabilities of each player’s winning the game given the pair of cards dealt. The entries in each cell of the table represent, for that pair of cards dealt, the number of cards (of the 50 remaining in the deck) for which the dealer would win (top), the opponent would win (middle), and the players would tie (bottom). The conditional probabilities of these events, given the pair of cards dealt, are therefore found by dividing these tabulated entries by 50.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
</tr>
</thead>
<tbody>
<tr>
<td>320</td>
<td>ROSSMAN AND TESMAN</td>
<td>321</td>
<td>DO YOU WANT TO DEAL?</td>
<td>320</td>
<td>ROSSMAN AND TESMAN</td>
<td>321</td>
<td>DO YOU WANT TO DEAL?</td>
<td>320</td>
<td>ROSSMAN AND TESMAN</td>
<td>321</td>
</tr>
</tbody>
</table>
In symbols, let \( W_D \) represent the event that the dealer wins the game, \( W_O \) that the opponent wins, \( T \) that a tie occurs, and \( C_{ij} \) that card \( i \) is dealt to the opponent and \( j \) to the dealer. Then
\[
\Pr(W_D) = \sum_{i,j} \Pr(W_D | C_{ij}) \times \Pr(C_{ij}) \\
\Pr(W_O) = \sum_{i,j} \Pr(W_O | C_{ij}) \times \Pr(C_{ij}) \\
\Pr(T) = \sum_{i,j} \Pr(T | C_{ij}) \times \Pr(C_{ij})
\]
where
\[
\Pr(C_{ij}) = \begin{cases} 
\frac{1}{52} & \text{for } i \neq j \\
\frac{1}{2} & \text{for } i = j.
\end{cases}
\]
These probabilities of the dealer winning the game, of the opponent winning the game, and of tying, assuming that each player uses his/her naive strategy, are as follows:

\[
\begin{align*}
\Pr(W_D) &= 0.4654 & \text{Dealer's Winning} \\
\Pr(W_O) &= 0.4685 & \text{Opponent's Winning} \\
\Pr(T) &= 0.0661 & \text{Tieing}
\end{align*}
\]

Since ties are to result in the game being replayed until one player wins, a player (eventually) wins the game by either winning after the first deal OR tying and then winning the second deal or tying twice and then winning the third deal OR . . . .

Thus, the probability of each player's (eventual) winning is found by determining the convergence of an infinite sum. In symbols, let \( W_D^* \) represent the event that the dealer eventually wins the game and \( W_O^* \) that the opponent eventually wins. Then
\[
\Pr(W_D^*) = \Pr(W_D) + \Pr(T) \Pr(W_D) + \Pr(T)^2 \Pr(W_D) + \cdots \quad \text{and}
\Pr(W_O^*) = \Pr(W_O) + \Pr(T) \Pr(W_O) + \Pr(T)^2 \Pr(W_O) + \cdots
\]
These are geometric series whose leading terms are \( \Pr(W_D) = 0.4654 \) and \( \Pr(W_O) = 0.4685 \), respectively, with a ratio of \( \Pr(T) = 0.0661 \). Thus, these probabilities are:
\[
\begin{align*}
\Pr(W_D^*) &= \frac{\Pr(W_D)}{1 - \Pr(T)} = \frac{0.4654}{1 - 0.0661} = 0.4983 \quad \text{and} \\
\Pr(W_O^*) &= \frac{\Pr(W_O)}{1 - \Pr(T)} = \frac{0.4685}{1 - 0.0661} = 0.5017.
\end{align*}
\]
In spite of the apparent advantages to the dealer, the opponent has a higher probability of winning the game than the dealer! The opponent's advantage, which slightly outweighs those for the dealer, comes from the fact that she never has to surrender a good card (since the initial decision to trade or not is hers), while the dealer may have to give up a good card if the opponent elects to trade. Note that the opponent has the advantage in both the upper right (where the opponent is dealt a good and the dealer a poor card) and the lower left (where the opponent is dealt a poor and the dealer a good card) portions of Table 4.1. In fact, of the \( 13 \times 13 = 169 \) possible pairs of cards to be dealt (which are not all equally likely, remember), the opponent has the advantage over the dealer in 87, the dealer over the opponent in 75, and neither has the advantage in 7. The answer to the 'Do you want to deal?' question seems less obvious in light of this analysis.

5. Other strategies. We have just seen that the opponent enjoys a slight advantage over the dealer if each player adopts the naive strategy of trading only when the probability of bettering one's card is at least as great as the probability of worsening it. Perhaps other strategies are better, though. For instance, maybe the dealer should be willing to trade with cards higher than a Seven if the opponent does not trade, for the opponent's action of not trading may indicate that she has a reasonably good card.

For the opponent, we consider all strategies of the form: trade with cards at and below \( N \) (for \( N = \text{Ace}, \text{Two}, \ldots, \text{Jack}, \text{Queen} \)), stick with cards above \( N \). For the dealer, we consider all strategies of the form: trade with cards at and below \( M \) (for \( M = \text{Ace}, \text{Two}, \ldots, \text{Jack}, \text{Queen} \)), stick with cards above \( M \). (Of course, we continue to assume that the dealer will do the only sensible thing if the opponent trades or has a King.) We consider these twelve different strategies for each player and conduct the analysis described above to determine the probability of each player's (eventual) winning of the game with that particular pair of strategies being used. Table 5.1 contains these probabilities for each of the 144 pairs of strategies. These are the probabilities of each player's (eventual) winning, so the entries in one table are simply 1 minus those in the other.

6. Analysis of different strategies. How should the players use the results in Table 5.1 to guide them in selecting strategies? One might start by eliminating dominated strategies; i.e., strategies which result in a lower probability of winning than another strategy no matter which strategy the other player selects (see, [1] or [3], for example). For the dealer, strategies \( M = \text{Ace}, \text{Two}, \text{Three}, \text{Four}, \text{Five}, \text{and Queen} \) are all dominated. (Remember that the form of the strategy is to trade with cards at and below \( M \), stick with cards above \( M \).) To see this, note that strategy \( M = \text{Six} \) dominates \( M = \text{Ace}, \text{Two}, \text{Three}, \text{Four}, \text{and Five} \); that the probability of the dealer winning with strategy \( M = \text{Six} \) exceeds that for each of the other dominated strategies for every strategy that the opponent might use. Also, dealer strategy \( M = \text{Queen} \) is dominated by strategy \( M = \text{Jack} \). For the opponent, strategies \( N = \text{Ace}, \text{Two}, \text{Three}, \text{Four, Eight, Nine, Ten, Jack, and Queen} \) are all dominated by strategy \( N = \text{Six} \) (for example). Thus, the principle of dominance eliminates from consideration many of the strategies available to each player. The dominated strategies are not worth considering since one can find a better strategy (i.e., one with a higher probability of winning) regardless of the other player's strategy.

The non-dominated strategies are \( M = \text{Six, Seven, Eight, Nine, Ten, and Jack} \) for the dealer, and \( N = \text{Five, Six, and Seven} \) for the opponent. Restricting consideration to these strategies results in the winning probabilities displayed in Table 6.1. Reapplying the dominance principle to these strategies allows us to eliminate the dealer's \( M = \text{Six, Nine, Ten, and Jack} \) strategies. Each of these is dominated by strategy \( M = \text{Eight} \) (for example). Once these dealer strategies are eliminated, the opponent should choose an \( N = \text{Seven} \) strategy. The dealer's best strategy against such an opponent is to play an \( M = \text{Eight} \) strategy. This pair of strategies is also the unique game-theoretic minimax strategy or Nash equilibrium for the game (see, [1] or [3]).

With the minimax approach, each player identifies, for each possible strategy, the
In general, the equilibrium need not exist and need not be unique when it does. "Mini-"

Opponent's probability of winning

Table 5.1

Probabilities of winning with various strategies

worst ("mini-") that he/she can do with that strategy. Then each player chooses the

Table 6.1

Probabilities of winning with non-dominated strategies

With this pair of strategies, the opponent has a .5007 probability of winning the game; there is no other strategy that assures her of a higher probability of winning regardless of the dealer's strategy. Likewise, there is no other strategy for the dealer that assures him of a higher probability of winning than .4993 regardless of the opponent's strategy. Notice that with these equilibrium strategies, the game still favors the opponent, but her advantage is less than that with the naive strategies, where her probability of winning is .5017.

One should not necessarily assume that the other player will play his/her equilibrium strategy. However, for example, if one knows that the other player is playing the naive strategy, a better strategy might be available. Table 5.1 reveals that if the opponent is playing her naive strategy (N = Six), the dealer's best strategy is M = Eight, which gives him a .5006 probability of winning. Thus, if the opponent plays her naive strategy, the dealer can actually have the advantage in the game by playing a better strategy than his naive one! On the other hand, if the dealer is known to be playing his naive strategy (M = Seven), Table 5.1 reveals that the opponent's best strategy is N = Seven, which gives her a .5063 probability of winning. Thus, the opponent can also do better than playing her own naive strategy against a naive dealer.

Finally, one can also discern from Table 5.1 that, while the game favors the opponent slightly, the worst that the opponent could possibly do is worse than the worst that the dealer could possibly do. By playing a ridiculous strategy (i.e., trading even with a card as good as a Queen), the opponent's probability of winning could plummet to as low as .3306. However, the dealer's probability of winning cannot sink below .4278, which would be achieved by adopting an M = Ace strategy (i.e., trading with an Ace but sticking with a Two or higher). Of course, the dealer's probability of winning could sink lower if he failed to make the only sensible decision when the opponent trades with him or reveals a King.

"Do you want to deal?" Probably not! A player armed with these results can achieve a higher probability of winning in the opponent's position, rather than in the dealer's position. If one believes, however, that his/her competitor will play ridiculous strategies, one can better exploit that foolishness from the dealer's position.

7. Conclusions.
We believe that this card game, despite being very simple to describe and to play, yields some surprising results and intriguing lessons about competitive strategies. The most surprising result has been that the game actually favors the opponent (an intelligent opponent, anyway), despite the rules which seem to offer several advantages to the dealer. More interesting, perhaps, is that the naive, shortsighted goal of seeking to improve one's card is not necessarily the best strategy to adopt. In fact, either player can have the advantage in the game by using a non-naive strategy if the other player is known to be using a naive one.

We recently discovered that this game goes by the name "le Her" and has been presented in some game theory books. (See [4].)

REFERENCES
ROSSMAN AND TESMAN


Allan J. Rossman, Department of Statistics, California Polytechnic State University, San Luis Obispo, CA 93407. arossman@calpoly.edu

Barry A. Tesman, Department of Mathematics and Computer Science, Dickinson College, Carlisle, PA 17013. tesman@ Dickinson.edu

Allan J. Rossman is an Associate Professor of Statistics. He is married and has two very spoiled but lovable cats, Eponine and Cosette. He enjoys playing tennis, managing a fantasy baseball team, traveling, and reading.

Barry Tesman is the Mathias Associate Professor of Mathematics at Dickinson College. He enjoys cycling, squash, and running. He is married and has two children, Emma and Lucy (also spoiled, but lovable).

Correction. In the last issue, due to a printer error, these diagrams were unreadable. They are Figures 2 and 3 in General Flip-Shift Games by Jae Gyun Cheong, Michael A. Jones and Kei Kaneko (IMPE Journal, Vol. 11, No. 5, pp 229 - 239, 2001).

PROBLEM DEPARTMENT

EDITED BY MICHAEL MCCONNELL, JON A. BEAL, AND CLAYTON W. DODGE

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 correspondence should be addressed to Michael McConnell, 840 Wood Street, Mathematics Department, Clarion University, Clarion, PA 16214, or sent by email to mmcconnell@clarion.edu. Electronic submissions using \LaTeX are encouraged. Please submit each proposal and solution preferably typed or clearly written on a separate sheet (one side only) properly identified with name, affiliation, and address. Solutions to problems in this issue should be mailed to arrive by December 1, 2002. Solutions identified as by students are given preference.

Problems for Solution.

1034. Proposed by Norman Schaumberger, Douglaston, New York
Let \(a, b, c \in \mathbb{Z}^+\). Show that
\[
\frac{(a + b + c) - a + b + c}{3} \geq \frac{(a + \frac{b + c}{2}) + \frac{a + b}{2}}{2}
\]

1035. Proposed by Ayoub B. Ayoub, Pennsylvania State University Abington College, Abington, Pennsylvania
Prove that if
\[
x = \sum_{k=1}^{2n+1} 2k-1 \left(\binom{2n+1}{k}\right)
\]
then \(\frac{1}{2}(x^2 - 1)\) is the product of two consecutive whole numbers.

1036. Proposed by Shiva Saksena, Univ. of North Carolina at Wilmington, Wilmington, North Carolina
Student solutions solicited.
Let
\[
f(x) = \prod_{n=0}^{\infty}(1 + x^{2n}).
\]
Find \(c\) such that
\[
\int_{0}^{c} f(x) \, dx = \pi.
\]

1037. Proposed by Jim Vandergriff, Austin Peay State University, Clarksville, TN
Evaluate
\[
\lim_{x \to \infty} \int_{0}^{x} \left(\frac{\ln x}{n}\right)^2 \, dx
\]
1038. Proposed by Dr. Shiva K. Saksena, University of North Carolina at Wilmington, Wilmington, North Carolina

Find all solutions of the equation

$$\ln(\log(x)) = \log(\ln(x)).$$

1039. Proposed by Cecil Rousseau, The University of Memphis

(Erdős) Let $n$ be a natural number. The number of odd divisors of $n$ equals the number of representations of $n$ as the sum of consecutive natural numbers. Note: Sums with one term are counted.

1040. Proposed by Andrew Cusumano, Great Neck, New York

Define $a_n = \sum_{i=0}^{n} \frac{1}{n+2i}$. Show that $\{a_n\}$ is a decreasing sequence and $\lim_{n \to \infty} a_n > \frac{1}{2}$.

1041. Proposed by Leon Bankoff, Los Angeles, California

The figure below shows a quarter circle with smaller circles inside.

1. Prove the three larger circles have radii of equal length.
2. Prove that the remaining six smaller circles also have radii of equal length.

1042. Robert C. Gebhardt, Hopatcong, N.J.

In a simple roulette game, there are thirty-six numbers, a predetermined half of the numbers are black and the other half are red.

1. In how many ways can the numbers be arranged in slots around the wheel if no two adjacent slits can have the same-colored number?
2. European roulette wheels also have a green 0. Repeat the question from part (1) for this situation.
3. American roulette wheels have a green 0 and a green 00. Repeat the question for this situation.

The poser writes: "In the small roulette wheel I own, presumably a ‘standard’ arrangement of the numbers, green 0 and green 00 are diametrically opposite each other. Also, adjacent numbers are diametrically across from each other: red 1 is opposite black 2, then black 13 is opposite red 14, then red 36 is opposite black 35, and so on, so the actual arrangement is more complicated than just avoiding having adjacent numbers of the same color."

1043. Mohd Nadeem Khan, New Abadi, Aligarh, India

Find all quadruples of distinct integers $x, y, u,$ and $v$ such that

$$xy = uv$$

1. $x - y = u + v$
2. $\gcd(x, y) = 1$
3. $\gcd(u, v) = 1$
4. $x > y$
5. $u > v$.

Solutions.

1007. [Spring 2001] Proposed by the editor.

As children, my siblings and I would eat great quantities of peanut butter. A favorite treat was (and still is) peanut butter on a banana. (Peel the banana first! Then put on the peanut butter.) Thus solve this base ten alphametic

$$\text{PEANUT} = \text{BUTTER} + \text{BANANA}.$$  

Solution by Cindy Mounce, student, Angelo State University, San Angelo, Texas.

Writing the alphametic vertically, we have

$$\begin{align*}
\text{BUTTER} + \text{BANANA} &= \text{PEANUT} \\
\text{B U T T E R} + \text{B A N A N A} &= \text{P E A N U T} \\
\end{align*}$$

There are eight possibilities for the carries involved in the hundreds and thousands columns. Suppose first we have no carries, that $T + A = N$ and $T + N = A$. By subtracting these two equations, we find that $A = N$, which is not possible. Similarly, if $1 + T + A = N + 10$ and $1 + T + N = A + 10$, then again $A = N$.

If $1 + T + A = N + 10$ and $T + N = A$, then by subtracting we get that $N - A = 1/2$, which is impossible in integers. Similarly, we cannot have $T + A = N + 10$ and $1 + T + N = A$, $T + A = N + 10$ and $1 + T + N = A + 10$, or $1 + T + A = N$ and $T + N = A + 10$.

Finally, we take $T + A = N$ and $T + N = A + 10$. Here $T = 5$ and $N = A + 5$. As above, all possibilities lead to contradictions except $E + N = U$ and $1 + U + A = E + 10$.

Now $U = E + 7$, $A = 2$, and $R = 3$, so $E < 2$. Since $E = 0$ yields $U = N$, we have $E = 1$ and $U = 8$. Since only 0, 4, 6, and 9 remain unused for $B$ and $P$, then $B = 4$ and $P = 9$. We have 912786 = 485513 + 427272, or

$$\begin{align*}
485513 &+ 427272, \\
912786 &
\end{align*}$$

Also solved by Charles D. Ashbacher, Charles Ashbacher Technologies, Hawahtas, IA, Paul S. Bruckman, Sacramento, CA, Rochelle Call, Viterbo University, Lacrosse, WI, Kenneth B.
There exist polynomials with integer coefficients that are irreducible over the field of rational numbers but are reducible over the field with respect to any prime modulus $p$. Prove that $f(x) = x^4 - 10x^2 + 1$ is such a polynomial.

I. Solution by H.-J. Seiffert, Berlin, Germany.

If $f(x)$ is reducible over the rationals, then it is reducible over the integers since its leading coefficient is 1. Since $f(x)$ has no integral zero, we must consider only the case $f(x) = (x^2 + ax + u)(x^2 + bx + v)$, where $a$ and $b$ are integers and $u$ and $v$ are rational.

If $u = 1$, then $a = 2\sqrt{3}$. If $u = -1$, then $a = -2\sqrt{3}$, so $f(x)$ is reducible over the rationals.

We prove $f(x)$ is reducible over $\mathbb{Z}_p$, the field of residues with respect to any prime $p$. It is easily checked that $f(x) = (x^2 + 1)^2$ in $\mathbb{Z}_p[x]$ as well as in $\mathbb{Z}_p$. So suppose $p > 3$.

If $f$ is a quadratic residue modulo $p$, then $a^2 \equiv 2 (\mod p)$ for some integer $a$ and $f(x) = (x^2 + ax + u)(x^2 - ax + 1)$. Similarly, if 3 is a quadratic residue modulo $p$, then $a^2 \equiv 3 (\mod p)$ for some integer $a$ and $f(x) = (x^2 + 2ax + 1)(x^2 - 2ax - 5)$.

If neither 2 nor 3 is a quadratic residue modulo $p$, then $f(x)$ is irreducible over $\mathbb{Z}_p$.

II. Comment by Rex H. Wu, Brooklyn, New York.

Lindsay Childs, in Problem E2578, The American Mathematical Monthly; Vol. 84, No. 5; May 1977, pp. 390-1, provided a proof to the theorem: Given any prime $p$ and integers $a$ and $b$, the polynomial $P(x) = x^4 - 2x^2 + b^2$ is reducible mod $p$.

Also solved by Paul S. Bruckman, Sacramento, CA, Koopa Tak-Lun Koo, Boston College, MA, J. Ernest Wilkins, Jr., Clark Atlanta University, GA, Rex H. Wu, and the Proposer.

1009. [Spring 2001] Proposed by Ice B. Risteski, Skopje, Macedonia.

a) Prove that if the polynomials $f(x)$ and $g(x)$ with integer coefficients are relatively prime over the field $\mathbb{Z}_p$ of residues with respect to the prime modulus $p$ and at least one of the leading coefficients is not divisible by $p$, then these polynomials are relatively prime over the field of rational numbers.

b) Show by way of an example that for any prime $p$ the converse assertion does not hold.

Solution by the Proposer.

a) Suppose $f(x)$ and $g(x)$ are polynomials with integral coefficients and where at least one leading coefficient is not divisible by the prime $p$, and suppose they have a common divisor $d(x)$ of positive degree over the field of rationals. Then the leading coefficient of $d(x)$ is not divisible by $p$, $f(x) = d(x)a(x)$ and $g(x) = d(x)b(x)$, where $a(x)$ and $b(x)$ are polynomials with rational coefficients. Since any polynomial with integral coefficients that factors over the field of rationals also factors over the integers, we may assume that all the coefficients are integers. Furthermore, since the leading coefficient of $f(x)$ or of $g(x)$ is not divisible by $p$, then neither can the leading coefficient of $d(x)$ be divisible by $p$. Passing to the field of residues modulo $p$, we see that $d(x)$ is of positive degree and is a divisor of $f(x)$ and $g(x)$ over that field.

b) The polynomials $x$ and $x + p$ are relatively prime over the field of rationals but actually equal over the field of residues modulo $p$.


Show that

$$\sum_{n=0}^{\infty} \left( \frac{e^n}{(n+1)^{n+1}} \right)^{\frac{1}{n+1}} - 2 \leq \frac{1}{2}$$

Solution by Doug Faires, Youngstown State University, Youngstown, Ohio.

The given inequality can be reexpressed as

$$e - 1 < \sum_{n=0}^{\infty} \left( \frac{e^n}{(n+1)^{n+1}} \right)^{\frac{1}{n+1}} < e$$

or by multiplying by $e$ and adjusting the index, as

$$e^2 - e < \sum_{n=1}^{\infty} \frac{e^n}{n^2} < e^2.$$

To show the left inequality in (1), consider the increasing function $f(x) = \ln x$, for $x \in [1, n]$, and the sequence $\{\ln n\}$ for $i = 1, 2, \ldots, n$. Since $\ln n > f(x)$ for $x \in [i-1, i]$, we have

$$\int_1^n \ln x \, dx = \sum_{i=1}^{n} \int_{i-1}^{i} \ln x \, dx < \sum_{i=1}^{n} \ln i = \sum_{i=1}^{n} \ln i = \ln n!.$$ 

Completing the integration and simplifying gives $\ln n! - \ln e^n + \ln e < \ln n!$ and $e/n! < (e/n)^n$. Summing the convergent series gives

$$e^2 - e = e(e - 1) = e \sum_{n=1}^{\infty} \frac{1}{n^2} < \sum_{n=1}^{\infty} \frac{e^n}{n^2}.$$ 

To show the right inequality in (1), first verify that

$$e < \frac{e^2}{2}, \quad \frac{e^2}{2} < \frac{e^3}{3}, \quad \frac{e^3}{3} < \frac{e^2}{2}, \quad \frac{e^4}{4} < \frac{e^3}{3}, \quad \text{and} \quad \frac{e^5}{5} < \frac{e^2}{2}.$$ 

When $n > 5$, $e^n < (n/2)^n$ implies that

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

Hence, for all $n \geq 1$, and with strict inequality for $n \neq 2$, $e^n - 1 < e \left( \frac{n}{2} \right)^n$ holds, and

$$\sum_{n=1}^{\infty} e^n < e \sum_{n=1}^{\infty} \frac{1}{2^n} = e^2.$$ 

Also solved by Brian Bradie, Christopher Newport University, Newport News, VA, Paul S. Bruckman, Sacramento, CA, Charles R. Diminnie, Angelo State University, San Angelo, TX.
Let $q$ be a perfect number. The square of a prime $p$ has only the one proper divisor $p$ and $p < p^2$. Any other positive integer $n > 1$ must have for proper divisors at least one pair $a$ and $b$ such that $n = ab$. So, if $q$ has more than 2 proper divisors, their product is greater than $q$. Suppose $q$ is odd. It is not known if such a number exists, but in "Unsolved Problems in Number Theory", 2nd edition, edited by Richard K. Guy, it is stated that there must be at least 29 (not necessarily distinct) prime factors, which of course are all greater than or equal to 3. It is then clear that the product of all the proper divisors of $q$ is greater than $q$. Therefore, no odd perfect number can satisfy the conditions.

If $q$ is an even perfect number, then it is well known that $q = 2^p - 1$, where both $p$ and $2^p - 1$ are primes. If $q$ has any proper divisors other than $2^p - 1$ and $2^p$, which occurs whenever $2^p - 1$ is composite, the conditions of the problem cannot be satisfied. Now, $2^p - 1$ is prime only when $p = 2$, so the only perfect number equal to the product of its proper divisors is $6 = 2^2 - 1$.

Also solved by Paul S. Bruckman, Sacramento, CA, Charles R. Diminnie, Angelo State University, San Angelo, TX, Doug Faires, Youngstown State University, OH, Richard I. Hess, Rancho Palos Verdes, CA, Peter A. Lindstrom, Batavia, NY, Yoshinobu Murayoshi, Okinawa, Japan, H.-J. Seiffert, Berlin, Germany, and J. Ernest Wilkins, Jr., Clark Atlanta University, GA, Rex H. Wu, Brooklyn, NY, and the Proposer.

1013. [Spring 2001] Proposed by Wu Wei Chao, He Nan Normal University, Xin Xiang City, He Nan Province, China.

Observe that $77 \times 88 = 6776, 77 \times 85 = 66066, 777 \times 858 = 6665566, 707 \times 8558 = 6050560, \text{ etc.}$ Prove that there exist infinitely many triples of palindromic natural numbers $x, y, z$ such that $xy = z$.

I. Solution by Mark Evans, Louisville, Kentucky.

Let $k$ be a positive integer and $x$ a palindrome of length exactly $k$ digits. Let

$$y = \sum_{i=0}^{n} 10^k$$

for any nonnegative integer $n$. Then $z = xy$ is simply the digits of $x$ repeated $n + 1$ times. This proves not only the problem posed, but goes further to prove that for any given palindrome $x$, there exist infinitely many palindromes $y$ such that $xy$ is a palindrome.

For example, if $x = 858$ and $n = 2$, then $z = 8858858858$.

II. Solution by William H. Peirce, Rangeley, Maine.

Let $x$ be the $n$-digit palindrome $111 \ldots 111$ and let $y = 11$. The product $z = xy = 1222 \ldots 2221$, an $(n+1)$-digit palindrome. Any product of palindromes that does not involve carrying, produces another palindrome. The more difficult problem is to find such palindrome-producing products of palindromes where carrying is involved.

III. Solution by Proposer.

Let $x = 99 \ldots 9$, $y = 5$. Then $xy = (10^n - 1)(5500 \ldots 0 - 55 = 549 \ldots 945$, for example. Also, since $7 \times 858 = 600667$ and $708 \times 8558 = 606660$, $707 \times 8558 = 606660$, it is easily seen that $70707 \ldots 070785 = 606660 \ldots 606066$.


Given in $\mathbb{R}^3$ an elliptic paraboloid, find the locus of the centers of the spheres which cut the paraboloid in two circles.

Solution by Proposer, with translation from the original Spanish by Gregorio Fuentes, Orono, Maine.

Place the paraboloid in the Cartesian plane so that it has the equation

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 2z,$$

and $a \geq b > 0$. It is a paraboloid of revolution if and only if $a = b$. Otherwise, $a > b$ and we let $c^2 = a^2 - b^2$. A plane perpendicular to the axis of the paraboloid, the $z$-axis, is in general an ellipse with major axis parallel to the $x$-axis, so in order to make that intersection a circle, it is necessary to tip the plane, leaving that major axis fixed. It follows that all circular sections of the paraboloid lie in two systems of parallel planes that coincide in case the paraboloid is of revolution. The plane of any such circle will be parallel to the $x$-axis and its center will lie in the $yz$-plane. It follows that the center of any sphere containing that circle also lies in the $yz$-plane. Of course, the intersection of a sphere and a plane always is a circle.

For the case $a = b$, the plane of any circle lying on the paraboloid is parallel to the $xy$-plane and its center is on the $z$-axis, the axis of the paraboloid, so the centers of all spheres that cut the paraboloid in two such circles lie on that axis. Since the radius of curvature of a plane curve $y = f(x)$ is given by

$$r = \frac{(1 + (y')^2)^{3/2}}{y''},$$

we see that for the parabola $2z = x^2/y^2$, the radius of curvature at $x = 0$ is $r = a^2$.

For the sphere to cut the paraboloid, but less than its height above the vertex. All such centers lie on the open halfline on the axis of the paraboloid originating at $(0, 0, a^2)$, and contained inside the paraboloid.

So we assume $a > b$. If two distinct surfaces $f(x, y, z) = 0$ and $g(x, y, z) = 0$ intersect in a curve and if $c$ is a constant, then $f + cg = 0$ is the equation of a surface through that curve of intersection. Consider the surface

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - 2z - S(x^2 + y^2 + (z - q)^2 - r^2) = 0$$

that one obtains from the intersection of our paraboloid and a sphere with appropriately chosen values for $q$ and $r$. By choosing $S = 1/a^2$, we eliminate $x$ and with a bit of algebra one finds that the equation reduces to a pair of planes $(cy + bz)(cy - bz) = 0$ when $r = q = a^2$. Then any plane that cuts the paraboloid in a circle must be parallel to one of these planes. Figure 1 shows the cross section in the plane $x = 0$ of the paraboloid and the planes $cy + bz = 0$ and $cy - bz = 0$. The segment of each line cut off by the parabola is a diameter of a circle cut from the paraboloid by the corresponding plane.

Since these two planes will not in the general case pass through the origin, their equations will be of the form $cy + bz + \lambda = 0$ and $cy - bz + \mu = 0$ for some constants $\lambda$ and $\mu$. Also, in the general case we let $(0, p, q)$ be the center and $r$ the radius of the sphere and we set

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - 2z - 1 = \frac{1}{a^2}(x^2 + (y - p)^2 + (z - q)^2 - r^2) = \frac{1}{a^2}b^2(cy + bz + \lambda)(cy - bz + \mu)$$

Since this equation is an identity, we can derive the following equalities by first multiplying through by $a^2b^2$ and then equating the coefficients of $y$ and of $z$, and the constants:

$$c(\lambda + \mu) = 2b^2p, \quad b(\mu - \lambda) = 2b^2q - 2a^2b^2, \quad \lambda \mu = -b^2p^2 - b^2q^2 + b^2r^2$$

These equations we solve for $\lambda$, $\mu$, and $r^2$ to obtain

$$\lambda = b \left( \frac{bp}{c} - (q - a^2) \right), \quad \mu = b \left( \frac{bp}{c} + (q - a^2) \right), \quad r^2 = \frac{a^2}{c^2}(p^2 + 2b^2q - a^2c^2).$$

Since the sphere is real, the square of its radius must be positive, so

$$p^2 + 2b^2q - a^2c^2 > 0$$

See Figure 2 for the trace in the $yz$-plane of the original paraboloid and the bounding parabola of Equation 3. Now, the points $(0, p, q)$ of Inequality 3 determine the exterior region of a parabola of axis $OZ$ and vertex $(0, 0, a^2/2)$, lying in the plane $x = 0$ and opening downward. We notice that this parabola cuts the paraboloid in the points $(0, \pm bc, c^2/2)$. On the other hand the normalized equations of the planes of the two
McCONNELL, BEAL, and DODGE

Fig. 2.

2 by + 2cz = c(a^2 + b^2)

-2by + 2cz = c(a^2 + b^2)

(0, -bc, c^2/2)

(0, bc, c^2/2)

y^2 = 2bc^2

y^2 + 2cz = a^2 + c^2

circles common to the sphere and the paraboloid are

0 = (cy + bz + \lambda)/a

0 = (cy - bz + \mu)/a

For these planes to cut the sphere, the distance from the center of the sphere to the planes is less than \( r \), and we recall that the distance from a point \( (p, q) \) to each of these lines is given by

\[ |(cy + bz + \lambda)/a|, \quad |(cy - bz + \mu)/a| \]

By setting each expression less than \( r \), we derive that

\[ 0 < -2bp + 2cq - c(c^2 + b^2) \]

\[ 0 < +2bp + 2cq - c(c^2 + b^2) \]

In the plane \( x = 0 \), these inequalities determine the interior in the positive \( z \)-direction of the angle whose vertex is \( (0, 0, (a^2 + b^2)/2) \) and whose sides have the slopes \( \pm b/c \). The lines bounding this angle are shown in Figure 2. The solution region that they determine is shown shaded.

Conversely, to any point \( (0, p, q) \) inside that angle there corresponds a sphere which has center at that point and radius \( r \), and we recall that the distance from a point \( (p, q) \) to each of these lines is given by

\[ |(cy + bz + \lambda)/a|, \quad |(cy - bz + \mu)/a| \]

\( 0 < -2bp + 2cq - c(c^2 + b^2) \)

\( 0 < +2bp + 2cq - c(c^2 + b^2) \)

As shown in Figure (a), the X pentomino can be 90% covered with six congruent tiles. (The shaded area is not covered by these tiles.) Design a tile so that three of them cover at least 85% of the X pentomino. Any of the tiles may be turned over, but they must not overlap each other or the border.

\( (x + y + z)^2 = (x^2 + y^2 + z^2) + 2xyz = \lambda a^2 \)

\( x + y + z = \lambda a \)

\( z = \lambda a - x - y \)

\( -2by + 2cz = c(a^2 + b^2) \)

\( 2by + 2cz = c(a^2 + b^2) \)

\( y^2 = 2bc^2 \)

\( y^2 + 2cz = a^2 + c^2 \)

Solutions by the Proposers.

The cross in Figure (b) above shows the best we could do, covering 85.3858% of the given pentomino. The shaded areas are not covered.

that annulus only. Let us consider the annulus formed by the circumcircle of radius $r$ and incircle of a regular $n$-gon. Let the common center be $O$, a side of the $n$-gon be $AB$ and the foot of the apothem to that side be $F$, as shown in the accompanying figure.

![Diagram of an annulus with center O, side AB, and foot of the apothem F.]

a) Since there are $n$ sides, then $\angle AOF = \angle FOB = \theta = \pi/n$ and the apothem $OF = r \cos \theta$. The area $K$ of the annulus then is $K = \pi r^2 - \pi (r \cos \theta)^2 = \pi r^2 (1 - \cos^2 \theta)$. The area of the $n$-gon is $n \cdot r \cos \theta \cdot r \sin \theta$, so the area of the region outside the $n$-gon and inside the outer circle is $R = \pi r^2 - nr^2 \sin \theta \cos \theta$. The desired ratio is then $R/K = (\pi r^2 - nr^2 \sin \theta \cos \theta)/[(\pi r^2 - \pi r^2 \sin^2 \theta)/(\pi r^2 \sin^2 \theta)]$. When $n = 3,$

$$R \quad K = \frac{\pi - 3\sqrt{3}/2}{\pi(\sqrt{3}/2)^2} = \frac{4\pi - 3\sqrt{3}}{3\pi} = \frac{4}{3} \sqrt{3}$$

b) Letting $x = \pi/n$, we see that $x \to 0$ as $n \to \infty$, so that the desired limit $L$ is

$$L = \lim_{n \to \infty} \frac{R}{K} = \lim_{x \to 0} \frac{x - \sin(x \cos x)}{x \sin^2 x}$$

which is indeterminate, so we apply L'Hopital's rule to get

$$L = \lim_{x \to 0} \frac{1 + \sin^2 x - \cos^2 x}{2 \sin x \cos x} = \lim_{x \to 0} \frac{2 \sin x}{2 \cos x + \sin x}$$

by replacing $1 - \cos^2 x$ by $\sin^2 x$ and dividing out a factor of $\sin x$ from numerator and denominator. One more application of L'Hopital's rule then yields

$$L = \lim_{x \to 0} \frac{2 \cos x}{-2x \sin x + 2 \cos x + \cos x} = \frac{2}{3}$$

II. Comment by Elizabeth Andy, Limerick, Maine.

After some twenty-odd years,

Time for a change now appears.

New editors lodge,

Replacing old Dodge.

Let's give them both twenty-odd cheers!

Though Dodge has written the column

And edited problems for all 'em,

The best praise is due

To each one of you

Who sent work from your cerebellum.

So stand, be counted, be bold,

And release the editor old.

Let's welcome the new

Men from Clarion who

Have settled down into the fold.

Also solved by Paul S. Bruckman, Sacramento, CA, Kenneth B. Davenport, Frackville, PA, Rob Downes, Mountain Lakes High School, NJ, Russell Euler and Jawad Sadek, Northwest Missouri State University, Maryville, Doug Faires, Youngstown State University, OH, Richard I. Hess, Rancho Palos Verdes, CA, G. Mavrigian, Youngstown State University, OH, Yoshinobu Murayoshi, Okinawa, Japan, Rex H. Wu, Brooklyn, NY, and the Proposer.

Editorial note. All other solvers found the area $R$ of the featured solution, noted that the area of each successive such region was $\cos^2 \theta$ times that of the preceding region, and summed the resulting infinite series to obtain an expression for the total shaded area. They then divided by the area $\pi r^2$ of the original circle, obtaining the same ratio as above or an equivalent form.


Consider Pascal’s triangle with the rows numbered $0, 1, 2, \ldots$. If the sum of all the elements above the $n$th row is a prime, characterize the number of elements in row $n - 1$.

Solution by Monte J. Zerger, Adams State College, Alamosa, Colorado.

Since the sum of the elements in row $k$ of Pascal’s triangle is $2^k$, it follows that the sum of all the elements above row $n$ is $2^n - 1$. If this number is a prime, it is a Mersenne prime and hence the exponent $n$, which also is the number of elements in row $n - 1$, is a prime.

Also solved by Frank P. Battles, Massachusetts Maritime Academy, Buzzards Bay, Brian Bradie, Christopher Newport University, Newport News, VA, Paul S. Bruckman, Sacramento, CA, George P. Evanovich, Saint Peter’s College, Jersey City, NJ, Mark Evans, Louisville, KY, Doug Faires, Youngstown State University, OH, Ovidiu Purdul, Western Michigan University, Kalmanan, Richard L. Hess, Rancho Palos Verdes, CA, Kenneth M. Wilke, Topeka, KS, Rex H. Wu, Brooklyn, NY, and the Proposer.


For a fixed number $k$, $0 < k < 1$, at each toss of a fair coin a gambler bets the fraction $k$ of the money he has at the moment. In the long run, what percentage of the tosses must he win in order to break even?

Solution by Brian Bradie, Christopher Newport University, Newport News, Virginia.

Each victory multiplies the gambler’s money by the factor $1 + k$, while each loss multiplies it by $1 - k$. Let $p$ denote the gambler’s long-term winning percentage. To break even, the gambler needs to have

$$(1 + k)^p(1 - k)^{1 - p} = 1.$$

Solving this equation for $p$ yields

$$p = \frac{\ln(1 - k)}{\ln(1 - k) - \ln(1 + k)}$$
It is interesting to note that as \( k \to 0, p \to 1/2, \) and as \( k \to 1, p \to 1. \)

Also solved by Paul S. Bruckman, Sacramento, CA, Mark Evans, Louisville, KY, Doug Faires, Youngstown State University, Ohi, Richard I. Hess, Rancho Palos Verdes, CA, J. Ernest Wilkins, Jr., Clark Atlanta University, GA, and the Proposer.


Eduard Lucas showed

\[
\frac{1^5 - 3^5 + 5^5 - \cdots + (-1)^{n+1}(2n - 1)^5}{1 - 3 + 5 - \cdots + (-1)^{n+1}(2n - 1)}
\]

is always a square number for every positive integer \( n \) but never a fourth power. Show that

\[
\frac{(1^7 - 3^7 + 5^7 - \cdots + (-1)^{n+1}(2n - 1)^7) - 28(1^3 - 3^3 + 5^3 - \cdots + (-1)^{n+1}(2n - 1)^3)}{1 - 3 + 5 - \cdots + (-1)^{n+1}(2n - 1)}
\]

is always a cube, but almost never a sixth power.

Solution by George P. Evanovich, Saint Peters College, Jersey City, New Jersey.

Let \( S_n \) denote the given expression. We shall prove that \( S_n = (4n^2 - 7)^3 \), which clearly is a cube for all integers \( n \). The difference between the two adjacent squares \((k+1)^2 \) and \( k^2 \) is the odd number \( 2k+1 \). Thus for \( 4n^2 - 7 \) to be a square, then \( 7 \) has to be an odd number or the sum of adjacent odd numbers, which occurs only for \( k = 3 \), that is, when \( n = 2 \), and then \( S_2 = 9^3 = 729 \). So \( S_n \) is never a sixth power except for \( n = 2 \).

We use mathematical induction to show that \( S_n = (4n^2 - 7)^3 \) for all positive integers \( n \). To that end, we have \( S_1 = (1 - 28)/1 = -27 \) and \( [4(1)^2 - 7]^3 = (-3)^3 = -27 \), so the statement is true for \( n = 1 \). Observe that

\[
S_{n+1} = \sum_{i=1}^{n} (-1)^{i+1}(2i - 1) = (-1)^{n+1}n.
\]

For the induction step we assume that \( S_n = (4n^2 - 7)^3 \) for some positive integer \( n \) and show that \( S_{n+1} = [4(n+1)^2 - 7]^3 \). Thus

\[
S_{n+1} = \sum_{i=1}^{n+1} (-1)^{i+1}(2i - 1)^3 - 28(2n + 1)^3 \sum_{i=1}^{n+1} (-1)^{i+1}(2i - 1)
\]

\[
= \sum_{i=1}^{n} (-1)^{i+1}(2i - 1)^3 - 28(2n + 1)^3 + (n+1)^3 \sum_{i=1}^{n} (-1)^{i+1}(2i - 1)^3 - 28(2n + 1)^3
\]

\[
= -n(4n^2 - 7)^3 + (2n+1)^3 - 28(2n + 1)^3 = [4(n+1)^2 - 7]^3
\]

by straightforward but rather tedious algebra.


1020. [Spring 2001] Proposed by M. V. Subbarao, University of Alberta, Edmonton, Alberta, Canada.

Dedicated to friend and colleague Murray S. Klamkin on his 80th birthday.

[Klamkin ably edited this Problem Department for 10 years until 1968 - ed.]

Let \( p_1, p_2, \ldots, p_r \) be \( r \) distinct odd primes and let \( a \) be any fixed integer. You are given that \((p_1 + a)(p_2 + a) \cdots (p_r + a) - 1\) is divisible by \((p_1 + a - 1)(p_2 + a - 1) \cdots (p_r + a - 1)\), which is trivially true for \( r = 1 \). Can it hold for any \( r > 1 \)? If so, give a specific example. A $100 award will be given for the first received valid example.

Remark 1. For \( a = 0 \), this is a known unsolved problem of D. H. Lehmer, Bull. Amer. Math. Soc. 38 (1932) 745-751. For \( a = 1 \), this also is an unsolved problem of mine in A Companion to a Lehmer Problem, Colloq. Math. Debrecen 52 (1998) 683-698.

Remark 2. One can also consider the more general problem obtained by replacing the primes \( p_1, p_2, \ldots, p_r \) by their arbitrary powers \( p_1^a, p_2^a, \ldots, p_r^a \). My conjecture here is that at least for the cases \( a = 0 \) or \( 1 \), we must have \( r = 1 \). See my joint paper with V. Sivaramanprasad, Some analogues of a Lehmer problem, Rocky Mountain J. Math. 15 (1985) 609-629.

Solution by Chetan Offord and Robert Wentz, Saint John's University, Collegeville, Minnesota.

We have a general solution for the case where \( r = 2 \). Consider any two primes \( p_1 \) and \( p_2 \) such that \( p_2 = p_1 + 2 \) and let \( a = -p_1 \). Then

\[
(p_1 + a)(p_2 + a) - 1 = (p_1 - p_1)(p_2 - p_1) = 1 = -1
\]

and

\[
(p_1 + a - 1)(p_2 + a - 1) = (p_1 - p_1 - 1)(p_2 - p_1 - 1) = -1 = -1.
\]

Of course, \(-1\) is divisible by \(-1\).

For a specific example let \( r = 2, p_1 = 3, p_2 = 5, \) and \( a = -3 \). Then, as above,

\[
(p_1 + a)(p_2 + a) - 1 = (3 - 3)(5 - 3) = 1 = -1
\]

and

\[
(p_1 + a - 1)(p_2 + a - 1) = (3 - 1)(5 - 3) = -1 = -1.
\]

Also solved by Paul S. Bruckman, Sacramento, CA, and Carl Libis, Assumption College, Worcester, MA.

Editorial note. A check for $100 was sent to Offord and Wente.
The 2000 National Pi Mu Epsilon Meeting

The Annual Meeting of the Pi Mu Epsilon National Honorary Mathematics Society was held in Madison, WI from August 2-3, 2001. As in the past, the meeting was held in conjunction with the national meeting of the Mathematical Association of America’s Student Sections.

The J. Sutherland Frame Lecturer was Thomas F. Banchoff from Brown University. His presentation was entitled “Twice as Old, Again, and Other Found Problems”.

Student Presentations. The following student papers were presented at the meeting. An asterisk(*) after the name of the presenter indicates that the speaker received a best paper award.

Miya Breen, Ohio Nu - University of Akron
Analyzing the Area of Fractal Tilings

Tonga Kim and Nancy Nichols, Virginia Iota - Randolph-Macon College
Can you Follow our “Train” of Thought?

Bob Shuttleworth, Ohio Xi - Youngstown State University
Quaternions

Lorna Salaman, via Illinois Alpha - University of Puerto Rico
Kairomone

Alison Ortong, Illinois Alpha - University of Illinois
Narnia

Tom Wakefield*, Ohio Xi - Youngstown State University
Factorizable Groups

Laura Hitt, Alabama Gamma - Samford University,
Divisibility Algorithms for Euclidean Rings

Barbara Chervenka, Texas Nu - University of Houston, Downtown,
Exploring Graph Theory through Conjectures of “Graffiti”

Enginda Onawan, Ohio Xi - Youngstown State University
Graph Theory: Decompositions

Camilla Smith, Michigan Alpha - Michigan State University
The Optimal Oriented Diameter of the 3x5 Torus and Joins of Graphs

Mohammed Aheuzad, Virginia Alpha - University of Richmond
On the Number Theory of Quaternions and Octonions

Teresa Selee, Ohio Xi - Youngstown State University
International Parity Relations and Real Interest Rates

Kathy Woodside*, North Carolina Gamma - North Carolina State University
Protecting the Public Health: Predicting PM Fine in Forsyth County

Joel Lepak, Ohio Xi - Youngstown State University
Cook’s Theorem

Nicole Miller, Maryland Zeta - Salisbury University
Periodicity and Long Term Evolution of Cellular Automata

Neda Khalidi and Jansen Peretin, Pennsylvania Upsilon - Duquesne University,
From Mathematics to Krypton: The Pursuit of Random Numbers

Eric Appelt*, Ohio Delta - Miami University
Bandwidth of a Product of Cliques of Uneven Size

Tracy Pekle, Ohio Delta - Miami University
Non-Euclidean Geometry from 1820 to 1920

Amy Joanne Herron, Ohio Delta - Miami University
Exploring Melodic Patterns in Diatonic and Chromatic Music

Call For Papers.

The next IME meeting will take place in Burlington, Vermont, August 1-3, 2002. See the IME webpage (http://www.pme-math.org/) for application deadlines and forms. Social events will include a tour of the Shelburne Museum, a Lake Champlain dinner cruise, and, of course, the IME banquet. See also the MAA webpage for details and for other activities in the Green Mountain State.
The MATHACROSTIC in this issue has been contributed by Dan Hurwitz.

a. A type of ellipsoid (2 wds.)

b. A technique to determine when two polynomials are identical (3 wds.)

c. The theorem may follow from this (2 wds.)

d. The clumsiest algorithm for ordering a set is to compare all others (3 wds.)

e. His test concerns infinite series convergence

f. Difference between prediction and perfection (3 wds.)

g. Favorite sequence of algebraists

h. Probabilist with a difficult name to spell

i. Function defined on any domain, for example (2 wds.)

j. You can measure this only if your scale is continuously calibrated (2 wds.)

k. Positions for the “internal clock” of a Turing machine

l. Result of applying a function

m. Statistical measure of spread

n. Greek who calculated the earth’s circumference

o. Ancient method for solving practical problems

p. Pi is an — the area of polygons inscribed in the unit circle (3 wds.)

q. Used to approximate roots of a function (2 wds.)

r. A step to be verified

s. Euclidean subgroup

t. Type of differentiation

u. Before edge identification, the form of the connected sum of two tori

v. Curriculum, half a century ago

w. Usual spelling of “prove” on exams

x. Usual spelling of “prove” on exams

y. Usual spelling of “prove” on exams

z. Usual spelling of “prove” on exams

Last month’s mathacrostic was taken from “Ten Misconceptions (about mathematics and its History)” by (Michael J.) Crowe.

"An entity, be it man or machine, possessing the deductive rules of inference and a set of axioms from which to start, could generate an infinite number of true conclusions, none of which would be significant. We would not call such results mathematics."

Jeanette Bickley was the first solver.
Contents

A Cyclotomic Determinant ............................................. 289
Ayoub B. Ayoub

Morley’s Triangle ..................................................... 293
Marcus Emmanuel Barnes

Cycles in Random Permutations ................................. 299
Wendy Corp, Theresa Friedman and Paul Klingsberg

An Infinite-Dimensional Lucas Matrix ....................... 307
Thomas Koshy

Randomly Generating a Finite Group ....................... 313
Kimberly L. Patti

Do you want to deal? .................................................. 319
Allan J. Rossman and Barry Tesman

Richard V. Andree Awards ........................................... 317
Meetings ................................................................. 342
From the Right Side ..................................................... 298
The Problem Department .............................................. 327
Edited by Michael McConnell, Jon A. Beal and
Clayton W. Dodge
Mathacroistic ............................................................ 344
Dan Hurwitz