Problem 1006

How many aces can be served?

The ΠME Journal

Volume 11, Number 3 Fall 2000

The ΠME Journal

Official Publication of the National Honorary Mathematics Society

The ΠME Journal is published biannually, once in the spring and once in the fall. Each volume consists of ten issues.

Current rates are as follows:

United States:	\$20 for 2 years
	\$40 for 5 years
Foreign:	\$25 for 2 years
Back issues:	\$5 each
Whole volume:	\$50 (5 years)
All back issues:	\$400 (1^{st} 10 volumes)

All subscription orders should be sent to the business manager.

Information for authors. Authors should send their submissions to the editor and should be prepared to submit final copies of their articles in LaTeXformat, with all figures as encapsulated postscript.

All articles are refereed. The ΠME Journal especially welcomes student written papers. Faculty submissions are held to the highest standards of interest, clarity and exposition.

Detailed instructions for authors can be found on the ΠME web pages at www.pme-math.org.

THE MATHEMATICS BEHIND A CARD TRICK

DANIEL J. ACOSTA AND LAREMY COWART*

Abstract. This article relates a common "pick a card" card trick and describes mathematically why it works.

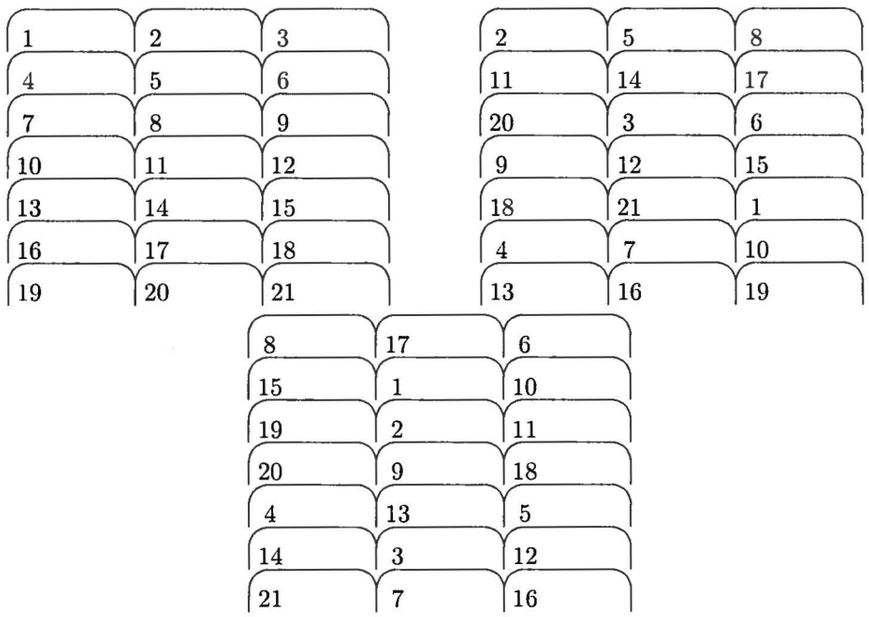


FIG. 0.1. *Our card trick where the chosen card is number 18*

1. A Card Trick. A. Deal out twenty one cards face up into seven rows each containing three cards. As you complete the first row, from left to right, begin the second row so that the new cards slightly overlap the cards in the first row. This will make the mechanics of the trick a bit easier.

B. After dealing out all seven rows in this manner, ask a bystander to silently select one of the twenty-one cards, telling you only the column (one, two, or three) that contains the card. From top to bottom, scoop up the cards in some other column, followed by the cards in the designated column which are stacked underneath the cards thus far, and finally the cards in the remaining column. Flip the deck over and repeat the dealing process in step A above.

C. Once more ask your volunteer which column now contains the card previously selected. Pick up the cards in the same manner as described above, again with the designated column picked up secondly. Repeat dealing one last time.

D. Inquire about the column one last time. The mystery card will be in the fourth position (the middle) of the column identified by your participant. Now what is a card trick without any sleight of hand? So instead of identifying the card verbally, show the card in grand style by following these steps: Pick up the columns as before

*Southeastern Louisiana University

(the secret card is of course in position eleven (the middle) out of the twenty-one card deck) and afterwards lay the first seven cards face down, one on top of the other. The next seven are laid atop this stack, each face down but only slightly overlapping one another, the cards alternately protruding from the top and bottom of the deck. The last seven cards are placed atop these, nice and flush just like the first seven. The result looks like a deck of cards with some of the middle cards sticking out the top and bottom. Picking up this bundle of cards with a firm grasp so that none of the protruding cards slip, gently pack the deck a few times on a firm surface allowing the middle cards to settle a bit. Pack from the other end now, and repeat this process, alternately packing from the bottom and top. All the middle cards should eventually settle flush with the rest of the deck with one card still protruding–the secret card occupying the middle position. You never even mention the card chosen by your patient friend. It appears!

We now unveil the secret of the trick and describe why the chosen card will always end up in the middle spot of the deck. We also generalize and ask what happens when the 7×3 pattern is replaced by a $k\times m$ pattern, $k, m \geq 2$. We wish to mention another article on this topic, recently brought to our attention [1].

2. A mathematical translation. Once the cards are dealt and a specific card chosen, the vertical position of the card in the designated column is denoted x, with $1 \leq x \leq k$ necessarily. When the cards are picked up in the aforementioned manner (always with the chosen column picked up next to last) then flipped and dealt, the same card is now in slot $\lceil \frac{k+x}{m} \rceil$ of some column, where $\lceil y \rceil$ denotes the smallest integer greater than or equal to y. To see this, note that after picking up the cards, the chosen card occupies position $k+x$ in the deck just before dealing, and by the Division Algorithm there is a unique $q \geq 0$ such that $k+x = q\cdot m + r$, $0 \leq r < m$. When $r = 0$ the card will appear in the last spot of the q^{th} row after the cards have been dealt again. If $r > 0$, the card appears in the r^{th} spot of the $(q+1)^{\text{st}}$ row. Either way, the new row housing the card is given by $\lceil \frac{k+x}{m} \rceil$, which necessarily lies between 1 and k, just like x. We have just completed step B of the card trick and have made use of the following function.

$$f : x \mapsto \left\lceil \frac{k+x}{m} \right\rceil$$

Iterating produces a dynamical system on the set of positive integers $\{1, 2, 3, 4, \ldots, k.\}$ We describe the end behavior of this system. For what follows, suppose $\frac{k}{m-1} \notin \mathbb{Z}$, but see comments afterwards.

1. There is a unique $s \in \{1, 2, 3, \ldots, k\}$, called the *stable element*, with the property that $f(s) = s$. In fact, $s = \left\lceil \frac{k}{m-1} \right\rceil$. This is the slot (in some column to be identified by the participant) eventually occupied by the mystery card.
2. All $x \in \{1, 2, 3, \ldots, k\}$ with $x < s$ satisfy $f(x) > x$. Similarly, all $x \in \{1, 2, 3, \ldots, k\}$ with $x > s$ satisfy $f(x) < x$. Therefore all x map to s after a certain number of iterations of f. The system is said to be *attracting*.
3. The minimal number of iterations, n, required for all elements to map to s depends upon m and k. In fact, $\lceil \log_m k \rceil - 1 \leq n \leq \lceil \log_m k \rceil + 1$. (Exact expressions for n are given in the proof.) Note we actually deal the cards $n+1$ times, as the first deal (step A) is not an iteration of f. Likewise, we've asked our participant to identify the column $n+1$ times (once after each deal).

In the case $\frac{k}{m-1} \in \mathbb{Z}$, there are two consecutive stable elements, $s_1 = \frac{k}{m-1}$ and $s_2 = \frac{k}{m-1} + 1$, the former attracting all $x \leq s_1$, the latter attracting all $x \geq s_2$.

3. Examples. We explicitly follow the map for our original 7×3 example under several iterations of f.

$$\begin{aligned}
1 &\mapsto 3 \mapsto 4\\
2 &\mapsto 3 \mapsto 4\\
3 &\mapsto 4 \mapsto 4\\
4 &\mapsto 4 \mapsto 4\\
5 &\mapsto 4 \mapsto 4\\
6 &\mapsto 5 \mapsto 4\\
7 &\mapsto 5 \mapsto 4
\end{aligned}$$

We thus see that after two iterations of f (steps B and C), the original row position x is mapped to the middle position, 4, irrespective of the initial value for x. Utilizing our notation in 2 and 3 of Section 2, we say for $k = 7$ and $m = 3$ we have $n = 2$ and $s = 4$, see Table 3.1. The data for $k \leq$ m can be similarly represented. In fact, $n = 1$

k	m	s	n	$\lceil \log_m k \rceil$	k	m	s	n	$\lceil \log_m k \rceil$
7	3	4	2	2	10	5	3	2	2
8	3	4,5	2	2	11	5	3	3	2
9	3	5	2	2	12	5	3,4	2	2
10	3	5,6	2	3	13	5	4	2	2
11	3	6	3	3	14	5	4	2	2
12	3	6,7	2	3	15	5	4	3	2
13	3	7	3	3	16	5	4,5	2	2
⋮	⋮	⋮	⋮	⋮	17	5	5	2	2
100	3	50,51	4	5	⋮	⋮	⋮	⋮	⋮
101	3	51	5	5	101	5	26	3	3
⋮	⋮	⋮	⋮	⋮	102	5	26	4	3
1000	3	500,501	6	7	103	5	26	4	3
1001	3	501	7	7	104	5	26,27	3	3
7	5	2	2	2	⋮	⋮	⋮	⋮	⋮
8	5	2,3	2	2	1000	5	250,251	5	5
9	5	3	2	2	1001	5	251	5	5

TABLE 3.1

or 2 for all such cases.

The examples in Table 3.2 demonstrate that the chosen card can be distinguished from a large number of cards in relatively few iterations.

4. Algebra of $\lceil y \rceil$. For the proofs that follow in section 5 we exploit the following properties of the smallest integer function. The proofs are left to the reader, but as a

k	m	s	n	$\lceil \log_m k \rceil$
100000	100	1011	3	3
1000000	100	10102	3	3
10000001	1001	100001	3	3

TABLE 3.2

hint, prove 3 first, using it in turn to prove 1.

$$\lceil x+y \rceil \leq \lceil x \rceil + \lceil y \rceil . \tag{4.1}$$

$$\lceil x-y \rceil \geq \lceil x \rceil - \lceil y \rceil . \tag{4.2}$$

$$\lceil x+n \rceil = \lceil x \rceil + n, \quad n \in \mathbb{Z}. \tag{4.3}$$

5. Proofs.

Proof. For the proof of result 1, recall $f : x \mapsto \lceil \frac{k+x}{m} \rceil$. The condition that $f(x) = x$ is thus

$$\begin{aligned} \left\lceil \frac{k+x}{m} \right\rceil = x &\Leftrightarrow x - 1 < \frac{k+x}{m} \leq x \\ &\Rightarrow mx - m < k + x \leq mx \\ &\Rightarrow (m-1)x < k+m \text{ and } k \leq (m-1)x \\ &\Rightarrow x < \frac{k+m}{m-1} \text{ and } \frac{k}{m-1} \leq x \\ &\Rightarrow \frac{k}{m-1} \leq x < \frac{k}{m-1} + \frac{m}{m-1} = \frac{k}{m-1} + 1 + \frac{1}{m-1} \end{aligned} \tag{1}$$

To prove that x is uniquely determined by this inequality it suffices, by the very last equality, to demonstrate $\frac{1}{m-1} \leq \left\lceil \frac{k}{m-1} \right\rceil - \frac{k}{m-1}$. In other words, $\frac{1}{m-1}$ is too small for $\left\lceil \frac{k}{m-1} \right\rceil$ and $\left\lceil \frac{k}{m-1} + \frac{1}{m-1} \right\rceil$ to be different integers. But this follows from:

$$\begin{aligned} \frac{k+1}{m-1} \leq \left\lceil \frac{k}{m-1} \right\rceil &\Rightarrow \frac{k+1}{m-1} - \frac{k}{m-1} \leq \left\lceil \frac{k}{m-1} \right\rceil - \frac{k}{m-1} \\ &\Rightarrow \frac{1}{m-1} \leq \left\lceil \frac{k}{m-1} \right\rceil - \frac{k}{m-1}. \end{aligned}$$

Note that here we explicitly use the assumption $\frac{k}{m-1} \notin \mathbb{Z}$ so that $\left\lceil \frac{k}{m-1} \right\rceil = \frac{k+p}{m-1}$, $p \geq 1$. Thus, there is exactly one integer satisfying (1), namely $s = \left\lceil \frac{k}{m-1} \right\rceil$. Note, for $k = 8, m = 3$, we have $s = 4, 5$. In all such examples where $\frac{k}{m-1} \in \mathbb{Z}$, two consecutive integers satisfy the double inequality (1). □

Proof. For the proof of result 2, suppose $x < s$, in fact, $x = s - t$. Then under our map f we observe the following:

$$\begin{aligned} x \mapsto \left\lceil \frac{k+x}{m} \right\rceil &= \left\lceil \frac{k+s-t}{m} \right\rceil \\ &= \left\lceil \frac{k+s}{m} - \frac{t}{m} \right\rceil \geq \left\lceil \frac{k+s}{m} \right\rceil - \left\lceil \frac{t}{m} \right\rceil = s - \left\lceil \frac{t}{m} \right\rceil \geq s - t = x. \end{aligned}$$

Note this last inequality is strict except for $t = 1$. Of course we don't need the strict inequality since by proof 1 above, $f(x) = x$ only happens for $x = s$. We also used the facts that s is stable under f and the function $\lceil x \rceil$ obeys a triangle inequality (see section 4).

An analogous argument shows $f(x) < x$ for $x > s$.

□

Proof. For the proof of result 3 we consider three cases.

Case 1: $m = 2$. Here, $s = \left\lceil \frac{k}{m-1} \right\rceil = k$ and thus after one iteration of f the numbers $k-1$ and k both map to k. We offer a more concrete interpretation. The two cards occupying position $k-1$ and k respectively in the column containing the selected card will occupy consecutive slots in the k^{th} row upon redealing (step B). Composing with f again produces a map that sends $k-3, k-2, k-1$, and k to k. In other words, the two cards sent to row $k-1$ after the first iteration are in the analogous position as the card in position $k-1$ mentioned above and thus will get sent to the k^{th} row upon redealing. Of course only one of these two cards actually ends up on the k^{th} row, namely the card in the same column as the selected card, but both cards have this potential and are thus counted, yielding a total of four original positions sent to k under two iterations of f. The next iteration will bring the total up to eight: two cards in each of the rows designated by the numbers previously mapped to k, namely, $k-3, k-2, k-2$, and k. In general then, after n iterations, 2^n elements have mapped to $s = k$. Solving the inequality $2^n \geq k$ gives us $n \geq \log_2 k$, so $n = \lceil \log_2 k \rceil$.

Case 2: $m = 3$. Here, $s = \left\lceil \frac{k}{m-1} \right\rceil = \lceil \frac{k}{2} \rceil$ and the same sort of argument as above shows that in the case k odd, 3^n positions map to position s after n iterations. It is important to note that the card occupying position s in the original column containing the selected card will be sent to the middle spot (middle row, middle column) in the card configuration after the first iteration so that the same number of positions map to s from above and below. This makes the calculation easy: $n = \lceil \log_3 k \rceil$. When k is even, we see that $\frac{k}{m-1} \in \mathbb{Z}$ and there are two s as mentioned above (Section 2). Upon the first iteration (redealing) these two positions of the original column now occupy positions $(\frac{k}{m-1}, 3)$ and $(\frac{k}{m-1} + 1, 1)$ respectively so that an equal number of positions map down to $s_1 = \frac{k}{m-1}$ as up to $s_2 = \frac{k}{m-1} + 1$. After n iterations then a total of $2 \cdot 3^n$ postions have mapped to either s_1 or s_2, so $2 \cdot 3^n \geq k$ yields $n = \lceil \log_3 \frac{k}{2} \rceil = \lceil \log_3 k - \log_3 2 \rceil = \lceil \log_3 k \rceil$ or $\lceil \log_3 k \rceil - 1$, (see the table in section 3 for both occurences.)

Case 3: $m \geq 4$. We first claim that $s = \left\lceil \frac{k}{m-1} \right\rceil \leq \frac{k}{2}$. To see this, note $\frac{k}{m-1} \leq \frac{k}{3}$ and thus it suffices to show $\lceil \frac{k}{3} \rceil \leq \frac{k}{2}$. Now, $\lceil \frac{k}{3} \rceil = \frac{k}{3}$, $\frac{k+1}{3}$, or $\frac{k+2}{3}$, each of which can be handled individually.

$$\begin{aligned} &\frac{k}{3} < \frac{k}{2} \\ &\frac{k+1}{3} = \frac{k}{3} + \frac{1}{3} < \frac{k}{3} + \frac{1}{2} = \frac{2k+3}{6} \leq \frac{3k}{6} = \frac{k}{2} \quad \text{for } k \geq 3. \\ &\frac{k+2}{3} = \frac{k}{3} + \frac{2}{3} < \frac{k}{3} + 1 = \frac{2k+6}{6} \leq \frac{3k}{6} = \frac{k}{2} \quad \text{for } k \geq 6. \end{aligned}$$

The reader can finish by explicitly checking the inequality for $k = 2, 3, 4, 5$.

Continuing to use our notation, we will count the number of iterations required for the chosen card to map to the s slot starting out at position $x = k$, i.e. the

last card in its column. This card is farthest away from position s ($\leq \frac{k}{2}$) and, as $f(k) \geq f(k-t)$, requires the most iterations to reach the stable position, thereby providing the minimum count n which we are seeking. After one iteration the s-card necessarily occupies position (s, r), where, as before, $k+s = mq+r$, $r < m$ by the Division Algorithm. Thus, the $l+1$ cards in position $s, s+1, s+2, \ldots s+l$ of the original column all mapped to row s under one iteration of f. Here l represents the quantity $m-r$. Under the next iteration then any card in row s, row $s+1, \ldots$ and row $s+l$ will all map to position s for a running total of $(l+1)m$ cards. In general, after n iterations a total of $(l+1)m^{n-1}$ cards have mapped to position s. We now solve for n required for the tally to reach $k-s+1$, i.e. the number of cards between s and k, inclusive, in the original column. Since $k-s+1 = (l+1)m^{n-1}$, we have $n = \lceil \log_m(k+1-s) - \log_m(l+1) + 1 \rceil \leq \lceil \log_m(k) + 1 \rceil \leq \lceil \log_m k \rceil + 1$, as claimed.

We can also get a lower bound for n. Claim: $n \geq \lceil \log_m k \rceil - 1$.

$$
\begin{aligned}
n &= \lceil \log_m(k+1-s) - \log_m(l+1) + 1 \rceil \\
&\geq \lceil \log_m(k+1-s) - \log_m(m+1) + 1 \rceil \\
&= \left\lceil \log_m\left(\frac{k+1-s}{m+1}\right) + 1 \right\rceil = \left\lceil \log_m\left(\frac{k+1-s}{m+1}\right) \right\rceil + 1 \\
&\geq \left\lceil \log_m\left(\frac{k+1-\frac{k(m-2)}{m-1}}{m+1}\right) \right\rceil + 1 \text{ (since } m \geq 4 \text{ and } s \leq \tfrac{k}{2}\text{)}, \\
&= \left\lceil \log_m\left(\frac{(k+1)(m-1)-k(m-2)}{m^2-1}\right) \right\rceil + 1 = \left\lceil \log_m\left(\frac{k+m-1}{m^2-1}\right) \right\rceil + 1 \\
&= \lceil \log_m(k+m-1) - \log_m(m^2-1) \rceil + 1 \\
&\geq \lceil \log_m(k+m-1) - \log_m(m^2) \rceil + 1 = \lceil \log_m(k+m-1) - 2 \rceil + 1 \\
&= \lceil \log_m(k+m-1) \rceil - 2 + 1 = \lceil \log_m(k+m-1) \rceil - 1 \\
&\geq \lceil \log_m k \rceil - 1
\end{aligned}
$$

□

REFERENCES

[1] J. Harrison, T. Brennan, S. Gapinski, *The Gergonne p−Pile Problem and the Dynamics of the Function* $x \mapsto \lfloor (x+r)/p \rfloor$, Discrete Appl. Math. **82** 103-113, (1998).

Daniel J. Acosta (dacosta2@selu.edu) and Laremy Cowart (istu24336@selu.edu), Department of Mathematics, Southeastern Louisiana University, Hammond, LA 70402.

Laremy Cowart is a junior computer science major at Southeastern Louisiana University. He has written code to generate fractal images and images of iterative processes such as Newton's Method. His interests include number theory and cryptography.

ΠΜΕ Journal, Vol. 11, No. 3, pp 123–124, 2000.

FACTORIZATION OF THE PRIMES

AYOUB B. AYOUB*

A prime number p has, by definition, no prime factorization other than the trivial one $p \cdot 1$. However, a prime number can be factored into numbers which do not belong to the ring of integers of the rational field. In this note, we will show that the odd prime number p has the factorization:

$$p = 2^{p-1} \cdot \sin^2\frac{2\pi}{p} \cdot \sin^2\frac{4\pi}{p} \cdot \sin^2\frac{6\pi}{p} \cdots \frac{(p-1)\pi}{p}$$

Although this result is interesting, it is the technique used to prove it, that is more significant. Here, the concept of a splitting field, which in this case is the cyclotomic field, will be used together with some facts from number theory.

For the proof, we will use the binomial equation $x^p - 1 = 0$. This is an equation whose roots are the p'th roots of unity. Since $x^p = \cos 2\pi r + i \sin 2\pi r$, then $x = (\cos 2\pi r + i \sin 2\pi r)^{1/p}$. When De Moivres Theorem is applied, we get

$$x = \cos\frac{2r\pi}{p} + i\sin\frac{2r\pi}{p} = e^{2r\pi/p}, \text{ where } r = 1, 2, 3, \ldots, p.$$

If we let $e^{2\pi r/p} = \omega$, then the roots of the equation are $1, \omega, \omega^2, \ldots, \omega^{p-1}$.

Now, $x^p - 1$ can be factored in two different ways, and we have

$$(x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1) = (x-1)(x-\omega)(x-\omega^2)\cdots(x-\omega^{p-1})$$

from which we get the identity

$$x^{p-1} + x^{p-2} + \cdots + x + 1 = (x-\omega)(x-\omega^2)\cdots(x-\omega^{p-1}) \tag{0.1}$$

The polynomial on the left side of (0.1) is called the p'th cyclotomic polynomial and is known to be irreducible over the rational field $\mathbb{Q}$. The right side, however, represents the factorization of the polynomial over the cyclotomic field $\mathbb{Q}(\omega)$, see [3].

Now, if we set $x = 1$ in (0.1), we get

$$p = (x-\omega)(x-\omega^2)\cdots(x-\omega^{p-1})$$

Each factor on the right can be shown to be a prime integer of the cyclotomic field $\mathbb{Q}(\omega)$, [1].

Since $\{1, 2, 3, \ldots, p-1\}$ is a reduced residue system (mod p), then $\{2, 4, 6, \ldots, 2p-2\}$ is also a reduced residue system (mod p), see [2]. Consequently $p = (x-\omega^2)(x-\omega^4)(x-\omega^6)\cdots(x-\omega^{2p-2})$.

Now, if we divide the factors by $\omega, \omega^2, \omega^3, \omega^{p-1}$, respectively, and notice that $\omega \cdot \omega^2 \cdot \omega^3 \cdots \omega^{p-1} = \omega^{p(p-1)/2}$, we get

$$p = (\omega^{-1} - \omega)(\omega^{-2} - \omega^2)(\omega^{-3} - \omega^3)\cdots(\omega^{1-p} - \omega^{p-1}).$$

Since $p - k \equiv -k \pmod p$, then to each factor there is another one with opposite sign; therefore

$$p = (-1)^{(p-1)/2}(\omega - \omega^{-1})^2(\omega^2 - \omega^{-2})^2(\omega^3 - \omega^{-3})^2 \cdots (\omega^{(p-1)/2} - \omega^{(1-p)/2})^2$$

*The Pennsylvania State University, Abington College

But $\omega^r - \omega^{-r} = 2i \sin \frac{2\pi r}{p}$

So, $p = (-1)^{(p-1)/2}(2i \sin 2\pi/p)^2(2i \sin 4\pi/p)^2(2i \sin 6\pi/p)^2 \cdots (2i \sin(p-1)\pi/p)^2$

After simplifying, we get

$$p = 2^{p-1} \sin^2(2\pi/p) \sin^2(4\pi/p) \sin^2(6\pi/p) \cdots \sin^2((p-1)\pi/p)$$

And now, we verify this result for $p = 3$ and $p = 5$.

If $p = 3$, we have $2^2 \sin^2(2\pi/3) = 4(\sqrt{3}/2)^2 = 3$, and if $p = 5$, we have $2^4 \sin^2(2\pi/5) \sin^2(4\pi/5) = 16((5+\sqrt{5})/8)((5-\sqrt{5})/8) = 5$.

One should bear in mind that factorization of a prime depends on the extension field $\mathbb{Q}(m)$ which contains that prime. For example, in the Gaussian field $\mathbb{Q}(i)$, the rational prime 5 can be factored into two Gaussian primes as $5 = (2-i)(2+i)$ while the prime 3 can not be factored because it is a Gaussian prime itself, see [3].

More information about this topic may be found in [2].

REFERENCES

[1] E. GROSSWALD, "Topics from the Theory of Numbers", The Macmillian Company. New York, 1966.

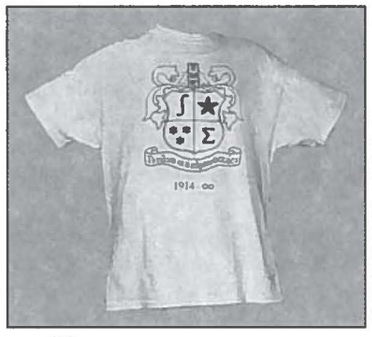
[2] I. NIVEN, H. ZUCKERMAN, and H. MONTGOMERY, "An Introduction to the Theory of Numbers", 5th ed. John Wiley and Sons. New York, 1991.

[3] H. POLLARD and H. DIAMOND. "The Theory of Algebraic Numbers", 2d ed. The Mathematical Association of America. Washington, 1975.

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

Ayoub B. Ayoub received his Ph.D. dregree from Temple University in 1980. His primary research interest is algebraic number theory. He is an active contributor to our problem department and has published extensively on a variety of teaching topics.

Hey, Sherlock Holmes didn't go without his hat....



ΠME Tee Shirts are white, Haines, BEEFY-T, pre-shrunk 100% cotton. The front has a large ΠME shield. The back of the shirt is decorated with the colorful ΠME tesselation of the plane designed by Doris Schattschneider, in the ΠME colors of gold, lavender and violet. Shirts are available in large and X-large. The price is only $10 per shirt, which includes postage and handling.

To obtain a shirt, send your check or money order, payable to ΠME, to:
Rick Poss,
Mathematics - ΠME
St. Norbert College
100 Grant St.
DePere, WI 54115

ΠME Journal, Vol. 11, No. 3, pp 125–133, 2000.

ELIMINATING FALSE POSITIVES IN A CRYPTOGRAPHIC METHOD *

ANNE MARIE DADDEA† AND MICHAEL A. JONES†

Abstract. Using a cryptographic method where two people exchange envelopes containing random numbers, it is possible to determine if they share confidential information without revealing the information. However, there is a possibility of a false positive; that is, there is a possibility that the people believe that they share the same information when they do not. A Monte Carlo simulation is used to determine the probability of a false positive. Restricting the random numbers can eliminate this problem without considerably comprising the random aspect of the procedure. Although the envelope method involves the addition of random numbers, multiplication could be used, as well.

1. Introduction. Cryptography can be used to determine if two people share confidential information without revealing it. This is the case if two people are trying to decide if they have the same person in mind while maintaining the confidentiality of that person's identity, such as two managers deciding whom to hire or fire. A similar situation could arise in a sexual harassment case where both the suspected harasser's and the victim's identity cannot be revealed. Likewise, it is important when discovering if two business associates know the same password for a computer program or two children know the same password for entry into a clubhouse. An article in The Economist [1] focuses on one method from an article by Fagin, Naor, and Winkler [2]. In their paper, they examine different methods for comparing confidential information.

Although Fagin, Naor, and Winkler pose several solutions to the problem, the technique examined in [2] utilizes only some paper, a pen or pencil, and a supply of envelopes - without any large prime numbers. The participants translate their information into a sequence of 0's and 1's through the use of a binary code. After writing down a set of random numbers, the participants sum the numbers in a subset determined by their binary sequences. If the participants' sums are the same, then the confidential information is believed to be the same. As discussed in [1] and [2], there is a possibility of a false positive; the sums are the same, but the information is different.

In Section 2, we review the envelope method and present examples, including a false positive. We determine the likelihood of a false positive through the use of a Monte Carlo simulation in Section 3. By restricting the set of numbers, we mathematically eliminate the possibility of a false positive. Although the numbers are no longer random, their arrangement is random. The large number of possible arrangements ensures the integrity of the restricted procedure. By noticing that the subset of the restricted numbers was more important than the numbers themselves, we eliminate the need to add the numbers. Instead, the participants compare two binary vectors; if the vectors are the same, then the paricipants share the same information. This mathematical development appears in Section 4. The approach in [2] can be modified by multiplying random numbers where identical products imply identical information. We consider such an approach in Section 5 and again eliminate the possibility of a false positive.

*This work was supported by a Student Faculty Research grant from the Office of Research and Sponsored Programs at Montclair State University.

†Montclair State University

2. The Envelope Method. To use the envelope method, the participants convert their information into binary form, using the same binary code. For this paper, we use the code in Figure 2.1. It consists of 5 binary digits in order to encode the 27

" "	0	0	0	0	0	I	0	1	0	0	1	R	1	0	0	1	0
A	0	0	0	0	1	J	0	1	0	1	0	S	1	0	0	1	1
B	0	0	0	1	0	K	0	1	0	1	1	T	1	0	1	0	0
C	0	0	0	1	1	L	0	1	1	0	0	U	1	0	1	0	1
D	0	0	1	0	0	M	0	1	1	0	1	V	1	0	1	1	0
E	0	0	1	0	1	N	0	1	1	1	0	W	1	0	1	1	1
F	0	0	1	1	0	O	0	1	1	1	1	X	1	1	0	0	0
G	0	0	1	1	1	P	1	0	0	0	0	Y	1	1	0	0	1
H	0	1	0	0	0	Q	1	0	0	0	1	Z	1	1	0	1	0

FIG. 2.1. *Encoding the alphabet.*

necessary characters, the 26 letters and a "space." We explain the envelope method through the following examples.

EXAMPLE 1. Assume that two managers want to determine if they want to hire the same applicant. Before applying the procedure, the managers must agree on restrictions on the number of letters to spell the applicants' names. In order to simplify the procedure, assume that the names of the applicants are at most three letters in length. The managers agree to fill the remaining characters after the name as "space" if they want to hire applicants whose names are less than 3 letters.

Assume that Manager A wants to hire "Rob" while Manager B wants to hire "Ed." Each manager translates the name of his top candidate into a binary sequence of 15 digits. The manager lists the sequence vertically and places random numbers in columns labeled 0 and 1. Both managers' encoded names and random numbers appear in Figure 2.2. Obviously, one manager's random numbers and encoded name

		0	1
	1	***4***	56
	0	***76***	24
R	0	16	***72***
	1	***81***	92
	0	3	***11***
	0	***1***	55
	1	***25***	64
O	1	19	***21***
	1	***70***	48
	1	***83***	37
	0	***71***	16
	0	***68***	82
B	0	***24***	40
	1	***12***	22
	0	***28***	6

		0	1
	0	13	***73***
	0	***85***	54
E	1	***30***	18
	0	5	***54***
	1	***92***	0
	0	***73***	23
	0	41	***99***
D	1	87	***60***
	0	28	***9***
	0	15	***69***
	0	***32***	77
	0	***95***	18
" "	0	***7***	26
	0	55	***35***
	0	***74***	82

FIG. 2.2. *Manager A's numbers (left) and Manager B's numbers (right) yield distinct sums and distinct names.*

are not observed by the other manager. Manager A and Manager B then add up the random numbers corresponding to their encoded names; these numbers are the boxed numbers from their own columns in Figure 2.2. Manager A's first sum is 627 and Manager B's first sum is 601.

The managers write their random numbers on separate slips of paper and seal the slips of paper in separate envelopes. The managers place their envelopes in two stacks, one for each of the 0's and 1's columns of random numbers, and keep the envelopes in sequential order - corresponding to the order in the columns. Hence, Manager A's fourth envelope in the 1's stack contains a slip of paper with the fourth number in the Manager A's 1's column. In our example, this envelope would contain "92."

The two managers exchange their stacks of envelopes. The managers open the envelopes that correspond to their binary sequence, returning the remaining envelopes that are then destroyed, in the presence of both managers. A count of the envelopes guarantees that the managers took the right number of envelopes. Each manager adds up the random numbers in the selected envelopes (as shown by the numbers in bold italics in the other managers' columns in Figure 2.2) and arrives at a second sum. Manager A's and Manager B's second sums are 887 and 647, respectively. After adding together both sums the managers reveal only their total sum. Manager A's grand total 1514 ($= 627 + 887$) and Manager B's grand total 1248 ($= 601 + 647$) are different. Since the totals are different, it follows that the names must be different, too. The managers do not have the same candidate in mind and can continue to discuss all of the candidates.

EXAMPLE 2. Assume the managers use the same random numbers as in Example 1, however, they both use the name "Ed." Again each party adds up the random numbers corresponding to his code as shown by the boxed numbers in Figure 3. Manager A's sum is 647 and Manager B's is 601. After sealing and exchanging the

		0	1
	0	***4***	56
	0	***76***	24
E	1	16	***72***
	0	***81***	92
	1	3	***11***
	0	***1***	55
	0	***25***	64
D	1	19	***21***
	0	***70***	48
	0	***83***	37
	0	***71***	16
	0	***68***	82
" "	0	***24***	40
	0	***12***	22
	0	***28***	6

		0	1
	0	***13***	73
	0	***85***	54
E	1	30	***18***
	0	***5***	54
	1	92	***0***
	0	***73***	23
	0	***41***	99
D	1	87	***60***
	0	***28***	9
	0	***15***	69
	0	***32***	77
	0	***95***	18
" "	0	***7***	26
	0	***55***	35
	0	***74***	82

FIG. 2.3. *Manager A's numbers (left) and Manager B's numbers (right) yield identical sums and identical names.*

envelopes, they add up the appropriate random numbers (those in bold italics from the other managers' columns). Notice that the boxed and bold, italic numbers are

identical. Manager A's second sum is 601 and Manager B's is 647. Once the two totals are combined and they reveal their grand totals, they discover that the grand totals are the same, 1248. They believe that the names are the same. And, in this case, they are right.

However, as indicated in [1] and [2], there is a possibility of a false positive. That is, it is possible that the grand totals of the managers are the same, but that the names are different. Indeed, we know that different subsets of numbers may add to the same value.

EXAMPLE 3. To demonstrate the possibility of a false positive, consider the random numbers used in Figure 2.4. Manager A adds the first sum of 627 to the

		0	1
R	1	94	56
	0	76	24
	0	16	72
	1	81	92
	0	3	87
O	0	1	55
	1	75	64
	1	19	21
	1	70	48
	1	83	37
B	0	71	16
	0	68	82
	0	24	40
	1	62	22
	0	28	6

		0	1
E	0	13	73
	0	85	54
	1	30	18
	0	5	54
	1	92	0
D	0	73	23
	0	41	99
	1	87	60
	0	28	9
	0	15	69
" "	0	32	77
	0	95	18
	0	7	26
	0	55	35
	0	74	82

FIG. 2.4. *Manager A's numbers (left) and Manager B's numbers (right) yield identical sums, but different names.*

second sum of 887 to yield 1514. Manager B adds the first sum of 601 to the second sum of 913 which also equals 1514. Since the totals are the same, they assume that the names are the same; however, in this case, the names are different and the sums are coincidentally the same because of the random numbers selected.

3. The Likelihood of False Positives. Before trying to eliminate the possibility of a false positive, we wanted to know how frequently false positives occur. If they don't occur very often, then we could accept the risk of using the envelope method without any modifications. By using a Monte Carlo simulation, we determined the likelihood of a false positive. For each iteration of the program, we assigned $2n$ random numbers to each manager; these numbers were positioned in two columns as in Figure 2.1. We assumed that Manager A had a fixed name, or fixed binary sequence of length n; we used the sequence of all 0's. We considered every possible binary sequence for Manager B. If the grand totals were equal for a sequence other than all 0's for Manager B, then this was considered a false positive. We ran this simulation determining the probability of a false positive for different values of n and for restrictions on the set of random numbers.

The probability of a false positive, as determined by the Monte Carlo simulation, appears in Figure 3.1. In Figure 3.1, the rows indicate a fixed range of values from

	1	2	3	4	5	6	7	8	9	10	11	12	13
2	37.19	74.7	93.42	98.23	99.35	99.79	99.94	99.98	99.99	100	100	100	100
4	17.24	41.19	68.39	88.2	95.93	98.45	99.5	99.8	99.91	99.94	99.95	99.99	99.99
8	8.3	21.06	39.74	63.72	83.84	94.28	98.05	99.26	99.72	99.87	99.91	99.98	100
16	4.11	10.91	22.38	39.27	59.45	80.1	92.4	97.37	98.93	99.63	99.85	99.94	99.98
32	2.27	5.58	11.05	21.62	36.29	56.46	76.03	90.57	96.41	98.71	99.41	99.74	99.9
64	0.97	2.69	5.64	11.42	19.93	34.17	53.62	74.57	89.3	95.75	98.42	99.3	99.73
128	0.5	1.42	2.96	6.08	10.51	18.95	32.22	51.6	72.19	87.93	95.38	98.33	99.09
256	0.29	0.73	1.55	2.87	5.04	9.71	17.45	30.14	47.91	69.39	85.85	95.07	97.91
512	0.16	0.4	0.78	1.56	2.65	4.86	9.43	16.62	29.36	46.25	67.81	85.2	94.4
1024	0.09	0.18	0.39	0.8	1.38	2.48	4.54	8.46	15.86	27.15	44.01	66.78	83.74
2048	0.08	0.14	0.25	0.39	0.79	1.31	2.38	4.48	8.07	14.91	26.07	42.64	64.06
4096	0.01	0.02	0.06	0.22	0.29	0.67	1.18	2.43	4.3	7.7	14.39	25.62	41.76
8192	0.01	0.02	0.06	0.12	0.23	0.44	0.57	1.14	2.11	4.03	7.46	13.83	23.8
16384	0	0	0.01	0.01	0.06	0.12	0.29	0.58	1.13	2.22	3.8	7.2	13.46
32768	0	0	0.01	0.02	0.02	0.11	0.23	0.38	0.7	1.46	2.69	5.93	11.66

FIG. 3.1. *Monte Carlo simulation results of the percent likelihood of a false positive for 1 to 13 bits of information and for random numbers drawn from* $\{0, 1, 2, \ldots, 2^n - 1\}$.

which random numbers were selected. In the row denoted 2^n, the random numbers were selected from the set of 2^n numbers, $\{0, 1, \ldots, 2^n - 1\}$. The columns fix the number of binary digits used by each manager. For each entry in Figure 3.1, the simulation was run for 10,000 sets of random numbers. As expected, the range of random numbers and the number of binary digits affects the probability of a false positive: increasing the range of the random numbers decreases the likelihood of a false positive, while increasing the amount of binary information increases the likelihood of a false positive. Even for only 13 binary digits, which is just shy of 3 letters in our binary code, the probability of a false positive is high for any reasonable restriction on the set of random numbers.

4. Eliminating False Positives. Increasing the range of random numbers does decrease the failure rate, but the numbers become too large to be manipulated easily. It would be ideal to modify the envelope method, eliminating the possibility of a false positive, while keeping the addition manageable.

To introduce the ideas and simplify the analysis, we examine all possible sums of the random numbers for one of the two managers. Our goal is to determine how to ensure that the sums generated by all binary sequences are distinct. Once one manager has $4n$ random numbers that guarantee distinct sums for sequences of length $2n$, then the first n rows of numbers could be used by Manager A while the second n rows of numbers could be used by Manager B. Both managers would have $2n$ random numbers and be able to use sequences of length n. This would guarantee that sums determined by the random numbers of both managers would be distinct unless the binary sequences were identical.

EXAMPLE 4. Assume that one person has 8 random numbers, 4 in each column. Again, the two columns could be labeled 0 and 1.

27	44
10	69
56	4
16	81

The 16 possible 4 digit binary sequences yield 16 distinct sums:

57, 74, 109, 116, 122, 126, 133, 139, 168, 174, 181, 185, 191, 198, 233, and 250.

There is no possibility of two binary sequences yielding the same sum using this set of random numbers.

To generate the numbers in Example 4, we altered the Monte Carlo simulation from Section 3. Is there a more natural way to guarantee that the numbers sum to distinct values? Further, is it possible to find "minimal" sums? In the previous example, the 16 sums ranged from 57 to 250. We can ensure distinct sums and reduce the range of the sums by restricting the numbers; the numbers will no longer be random, but will be placed in a random order. If a manager selects either 0 or a different 2^k for $k = 0$ to $n-1$ for the entries in the n rows, as in Example 5, then she can ensure that binary sequences yield distinct sums. This idea is used to eliminate false positives by having one manager use 2^k for $k = 0$ to $n-1$, while the other manager uses 2^k for $k = n$ to $2n-1$.

EXAMPLE 5. Assume that a manager places a 0 and a different 2^k for $k = 0$ to 3 in each row, as below,

$$\begin{matrix} 0 & 4 \\ 2 & 0 \\ 0 & 8 \\ 0 & 1. \end{matrix}$$

All possible 4 digit binary sequences yield 16 distinct sums:

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, \text{ and } 15.$$

These possible sums are minimal because they consist of the 16 consecutive integers between 0 and 15.

The above example eliminated the possibility of a false positive for a single manager; that is, it guaranteed that all possible binary sequences yielded distinct sums of the manager's own numbers. Before applying this idea to two managers, as was described previously, the example is extended and shown to eliminate false positives for any number of bits.

THEOREM 4.1. *For the two columns of numbers,*

$$\begin{matrix} 0 & 1 \\ 0 & 2 \\ 0 & 4 \\ 0 & 8 \\ \vdots & \vdots \\ 0 & 2^{n-1} \end{matrix}$$

all possible binary sequences of length n generate distinct sums of the consecutive integers between 0 and $2^n - 1$.

Proof. This is a proof by mathematical induction on the n binary digits. For $n = 1$, the columns and sums are equal to equal 0 and 1. These sums are distinct and minimal.

Assume the following $n-1$ rows yield sums that are the consecutive integers from

0 to $2^{n-1} - 1$:

$$\begin{matrix} 0 & 1 \\ 0 & 2 \\ 0 & 4 \\ 0 & 8 \\ \vdots & \vdots \\ 0 & 2^{n-2} \end{matrix}.$$

Adding another row to accomodate another binary digit is equivalent to adding a 0 or 2^{n-1} to the possible sums from the first $n-1$ pieces of binary information.

If adding 0, then the sums remain the same: $0, 1, 2, 3, \ldots$, and $2^{n-1} - 1$. If adding 2^{n-1}, then the sums equal $2^{n-1}, 2^{n-1}+1, 2^{n-1}+2, 2^{n-1}+3, \ldots$, and $2^{n-1}+2^{n-1}-1 = 2^n - 1$. The sums are distinct and minimal. Hence, it is true for every value of n. □

Although this is a valid way to eliminate two sequences yielding the same sum, restricting the numbers to such an extent damages the random aspect of the method. Eliminating the random numbers hurts the integrity of the method, since manager's know what numbers the other manager uses. On the other hand, even though the numbers are restricted, they can still be arranged in a random order.

For n rows, there are $2^n n!$ ways to arrange a 0 and a distinct 2^k, for $0 \leq k \leq n-1$, in every row. Since k is an integer between 0 and $n-1$, inclusive, there are n values of k and $n!$ ways to determine which value of k appears in which row. For each row, the 0 can appear in either column. Since there are n rows, the 0's can be arranged in 2^n ways. Hence, there are $2^n n!$ ways to arrange a 0 and a distinct 2^k in n rows.

To emphasize the large number of arrangements, realize that for a 3 letter word or 15 binary digits, there are $2^{15}15!$ or 4.28×10^{16} arrangements of 0's and distinct values of 2^k. And, of course, all arrangements yield distinct and minimal sums.

So far the method for eliminating false positives has concentrated only on the random numbers of one manager. This idea can be extended to both managers if different powers of two are assigned to each. For n binary digits, one manager can use integer values for k between 0 and $n-1$, while the other manager uses integer values between n and $2n-1$. This will ensure distinct and minimal sums. There are $2^{2n} n! n!$ ways to arrange the numbers.

EXAMPLE 6. If each manager selects numbers with a 0 and a 2^k in each row and Manager A selects numbers where $0 \leq k \leq 14$ and Manager B selects numbers where $15 \leq k \leq 29$, they arrange those numbers in a random manner as in Figure 6. Manager A's own sum is 22523 and Manager B's is 190644224 (adding the manager's own boxed numbers). After sealing and exchanging the envelopes they add up the appropriate numbers and Manager A's sum using Manager B's numbers is 272924672 and Manager B's sum using Manager A's numbers is 9153 (adding the other manager's bold numbers). Manager A adds 22523 to 272891904 which equals 272914427 and Manager B adds 190644224 to 9153 which equals 190653377.

Although this eliminates the false positive by yielding distinct and minimal sums, the numbers are large and the sums are cumbersome. The same idea can be simplified using vectors. Rather than writing 2^k as an integer in each row, we could leave the integers as powers of 2. Therefore, the numbers in Figure 5 could be changed from 32 to 2^5, *etc.* Adding the boxed numbers of $32+2+16384+\ldots+256$ for Manager A can be written as: $1 \cdot 2^5 + 1 \cdot 2^1 + 1 \cdot 2^{14} + \ldots + 1 \cdot 2^8$. Similarly, the sum of Manager B's boxed numbers is: $1 \cdot 2^{20} + 0 \cdot 2^{26} + 1 \cdot 2^{19} + \ldots + 0 \cdot 2^{21}$. The coefficient of 0 or 1 for each 2^k indicates whether that power of 2 is part of the sum of their encoded

		0	1
	1	***0***	32
	0	***2***	0
R	0	16384	***0***
	1	***0***	16
	0	128	***0***
	0	***0***	2048
	1	***0***	512
O	1	0	***8***
	1	***8192***	0
	1	***0***	4096
	0	***64***	0
	0	***1***	0
B	0	***0***	4
	1	***0***	1024
	0	***256***	0

		0	1
	0	1048576	***0***
	0	***0***	67108864
E	1	***0***	524288
	0	33554432	***0***
	1	***32768***	0
	0	***0***	536870912
	0	134217728	***0***
D	1	0	***4194304***
	0	65536	***0***
	0	16777216	***0***
	0	***262144***	0
	0	***0***	131072
" "	0	***0***	8388608
	0	0	***268435456***
	0	***0***	2097152

FIG. 4.1. *Manager A's numbers (left) and Manager B's numbers (right) are distinct powers of 2.*

information. The same is done with the numbers in bold italics so that both Manager A and Manager B have their combined sums represented by either a 0 or a 1 times 2^k, for every k.

The manager's sums are translated into a $(0,1)$-vector by considering each power of 2 as part of a basis. The k^{th} entry of the vector indicates whether 2^k is part of the sum. To determine whether the names are the same, the managers need only compare their vectors. For Example 6, Manager A's vector is

$$(1,1,0,1,1,1,1,1,1,1,1,0,1,0,1,1,0,0,1,0,0,0,1,0,0,0,0,0,1,0)$$

and Manager B's vector is

$$(1,1,0,1,0,0,1,0,1,0,0,0,0,1,0,0,1,0,0,1,0,1,1,1,0,1,0,1,1,0,1,0,1,0,0).$$

Since the vectors are not identical, the names are different.

In general, a sum looks like $a_0 2^0 + a_1 2^1 + a_2 2^2 + \ldots + a_{2n-1} 2^{2n-1}$ where $a_i = 0$ or 1. The vector $\mathbf{a} = (a_0, a_1, \ldots, a_{2n-1})$ contains the same information as the sum. To recap, the managers begin by changing a word into a binary sequence. This binary sequence is converted to a sum by adding different powers of 2, which is then converted back into a binary sequence!

The middle process can be eliminated and the managers can flip and permute the bits of the original encoded message; flipping and permuting bits is a one-to-one function. Manager A's function can be determined given the arrangement of the powers of 2 in the two columns. To demonstrate, consider Manager A's columns of numbers from Example 6 where $\mathbf{a} = (a_0, a_1, \ldots, a_{14})$ is Manager A's original sequence. The process of adding the different values and changing back into a $(0,1)$-vector is represented by the map

$$f(\mathbf{a}) = (a_{11}^*, a_1, a_{12}, a_7, a_3, a_0, a_{10}^*, a_1^*, a_{14}^*, a_6, a_{13}, a_5, a_9, a_8^*, a_2^*)$$

where $a_k^* = 0$ if $a_k = 1$ and $a_k^* = 1$ if $a_k = 0$.

Additionally, Manager B's random assignment of powers of 2 can be determined by a one-to-one function g. If $\mathbf{a}$ and $\mathbf{b}$ are Manager A's and Manager B's original sequences then Managers A and B compare the following vectors of length $2n$: $(f(\mathbf{a}), g(\mathbf{a}))$ and $(f(\mathbf{b}), g(\mathbf{b}))$. The swapping of envelopes is equivalent to swapping functions. Manager A adds up numbers from the Manager B's columns to determine the image of $\mathbf{a}$ under Manager B's function; Manager B makes a similar computation. If the vectors are the same, then the original information is the same, too.

5. A Multiplicative Approach. Adding numbers and guaranteeing distinct sums is a bit harder than multiplying numbers and guaranteeing distinct products. The envelope method can be modified to use the multiplication of random numbers, as opposed to the addition of random numbers. If every number is restricted to be a distinct prime, then the products are distinct. To restrict the size of the products, in every row, a manager places a 1 in one column and a prime in the other column. Manager A selects primes below a certain value and Manager B selects primes above a certain value. By the fundamental theorem of arithmetic [3], if the products are the same then they factor uniquely. Since the primes appear at most once, when the products are the same, then the names are the same.

Of course, we need not worry about running out of primes. However, the technique to guarantee distinct sums above can be used to guarantee distinct powers of primes, as in the following example.

EXAMPLE 7. Assume the following two columns of numbers are used for the multiplicative variant of the envelope method.

$$\begin{matrix} 1 & 3^{2^0} \\ 1 & 3^{2^1} \\ 1 & 3^{2^2} \\ 1 & 3^{2^3} \end{matrix}.$$

By Theorem 4.1, all possible binary sequences of length 4 yield 16 distinct products: $3^0, 3^1, 3^2 \ldots, 3^{14}$, and 3^{15}.

As in the additive approach, the possibility of a false positive has been eliminated. And, as in Section 4, there are $2^n n!$ ways to arrange the numbers.

REFERENCES

[1] *Swap you.* The Economist, February 7, 1998, p 83.

[2] FAGIN R., NAOR M. AND WINKLER P., *Comparing Information Without Leaking It*, Communications of the ACM, Vol. 39, pp 77-85, 1996.

[3] NIVEN I. and ZUCKERMAN H. S., "An Introduction to the Theory of Numbers", John Wiley & Sons, 1980.

Anne Marie Daddea (AnnMD98@aol.com) and Michael A. Jones (jonesma@pegasus.montclair.edu), Department of Mathematical Sciences, Montclair State University, Upper Montclair, NJ 07043.

Anne Marie Daddea is an undergraduate student of mathematics education. She worked on this research during the summer between her sophomore and junior years. She has guest lectured and taught this material to undergraduate students in a course satisfying the general education requirements at Montclair.

Michael A. Jones' (Ph.D. 1994) research interests include mathematical psychology, economics, and political science. He is happy that this article stems from an article in his favorite publication, "The Economist".

ΠME Journal, Vol. 11, No. 3, pp 135–137, 2000.

THE DETERMINANT OF A (M, N) PRETZEL*

NITISH DASS, JONATHAN MCGRATH AND ERIN URBANSKI

Abstract. We prove that the determinant of a (m,n) pretzel knot or link is $m+n$ when $n, m > 0$.

1. Introduction. For any k-tuple of integers, define a $(m_1, m_2, \cdots, m_k)$ *pretzel* to be the knot or link with $|m_1| + |m_2| + \cdots + |m_k|$ crossings formed as illustrated below.

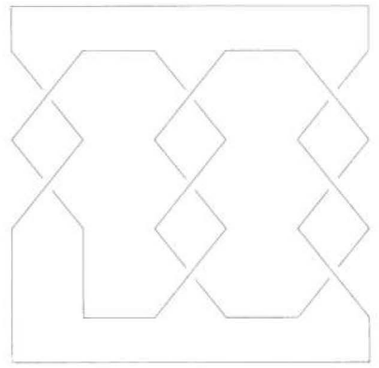


FIG. 1.1. *A* $(2,3,-3)$ *pretzel.*

The determinant of a knot or link is the absolute value of the determinant of a matrix associated with the knot or link. It is well known that the determinant is a knot/link invariant [1, Theorem 5, p. 46). In this paper we will prove the following result.

THEOREM 1.1. *The determinant of a* (m,n) *pretzel is* $m+n$ *when* $m, n > 0$.

The proof of the theorem depends on a precise labeling scheme for a (m,n) pretzel. In section 2 we will describe the labeling scheme; in section 3 we will show how to set up the associated matrix; in section 4 we will compute the determinant of the matrix; and in section 5 we conclude with conjectures about other pretzels.

2. The Knot. We begin with a systematic method for labeling each crossing and each arc on an (m,n) pretzel. To label the crossings, we start with the upper left most crossing and assign it the number 1. Then moving counterclockwise, we label successive crossings 2, then 3, and so on up to the final crossing which is labeled $m+n$. We follow a systematic labeling scheme for the arcs as well. The uppermost arc is labeled x_1. Then at the nth crossing, the overlapping arc is labeled x_{n+1}. Continue in this manner until all arcs have been labeled. See Figure 2.

3. The Matrix. A $k \times k$ matrix can be associated with any knot or link whose projection has k crossings. Rows of the matrix correspond to the crossings of the knot and columns correspond to the arcs.

*St. Olaf College

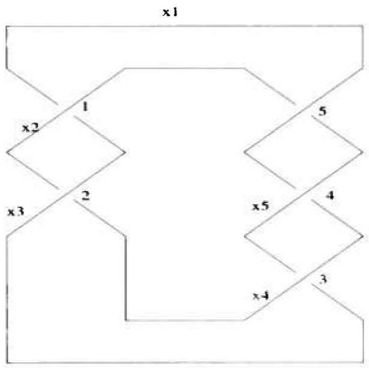


FIG. 2.1. *A labeled* $(2,3)$ *pretzel.*

Consider the ith crossing. In row i, place a 2 in the column corresponding to the overlying arc, place -1's in the columns corresponding to the two underlying arcs, and place zeros everywhere else. Follow this procedure for each of the k crossings.

The labeling scheme assures that at the ith crossing, the overlying arc is x_{i+1} and the underlying arcs are x_i and x_{i+2}. The $(m+n)\times(m+n)$ matrix for any (m,n) pretzel with the given labeling scheme basically follows a diagonal pattern of -1's on the main diagonal, 2's on the superdiagonal, followed by another diagonal of -1's. All other entries are 0's. See Figure 3.

$$\begin{bmatrix} -1 & 2 & -1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & -1 & 2 & -1 & 0 & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & & & & & & \cdot \\ \cdot & \cdot & & \cdot & & & & & \cdot \\ \cdot & \cdot & & & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot & & & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & -1 & 2 & -1 \\ -1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & -1 & 2 \\ 2 & -1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & -1 \end{bmatrix}$$

FIG. 3.1. *The matrix for a* (m,n) *pretzel.*

4. The Determinant. Now that the matrix has been established the determinant can be computed. The determinant of the knot is the absolute value of the determinant of the submatrix obtained by eliminating any one row and any one column of the original matrix (1, Theorem 4, p. 45). We will cross off the last row and first column of the matrix for a (m,n) pretzel. This gives a $(n+m-1)\times(n+m-1)$ matrix. For simplicity we will let $p=m-1$ giving a $(n+p)\times(n+p)$ matrix.

To help us compute the determinant, we will reduce the matrix to echelon form. We begin by successively interchanging the first and second row, then the second and third row, etc. This continues $n+p-1$ times until the original first row becomes the last row. The subsequent matrix is in row echelon form except for the last row, which is of the form $[2\ -1\,0\cdots0]$.

Let R_j denote row j. Perform the row operation which replaces row R_{n+p} with $2R_1+R_{n+p}$ so that the last row is of the form $[0\,3\ -2\,0\cdots0]$. This process continues: successively replace row R_{n+p} with $iR_{i-1}+R_{n+p}$ so that at each step the last row becomes $[0\,0\cdots(i+1)\,(-i)\,0\cdots0]$, where the entry $i+1$ is in the $(n+p,i)$ position and the entry $-i$ is in the $(n+p,i+1)$ position. The final operation will replace R_{n+p} with $(n+p)R_{n+p-1}+R_{n+p}$ so the last row becomes $[0\,0\cdots0\ -(n+m)]$. The resulting matrix is seen in Figure 4.

$$\begin{bmatrix} -1 & 2 & -1 & 0 & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & -1 & 2 & -1 & 0 & \cdot & \cdot & \cdot & 0 \\ & & \cdot & & & & & & \\ \cdot & \cdot & & \cdot & & & & \cdot & \cdot \\ \cdot & \cdot & & & \cdot & & & \cdot & \cdot \\ \cdot & \cdot & & & & \cdot & & \cdot & \cdot \\ & & & & & & \cdot & & \\ 0 & & & \cdot & \cdot & \cdot & -1 & 2 & \\ 0 & & & \cdot & \cdot & \cdot & 0 & -(n+m) & \end{bmatrix}$$

FIG. 4.1. *The row reduced matrix for a* (m,n) *pretzel.*

The determinant of the matrix in reduced echelon form shown in Figure 4 is the product of the entries along the main diagonal, $(-1)^{n+p-1}(n+m)$. Row operations which replace R_{n+p} with $iR_{i-1}+R_{n+p}$ do not alter the value of the determinant. Moving the first row to the last changes the value of the determinant by a factor of $(-1)^{n+p-1}$. Thus, the determinant of the original matrix is $(-1)^{n+p-1}(-1)^{n+p-1}(n+m)=n+m$, and Theorem 1 is proved.

5. Conjectures and Problems. CONJECTURE 5.1. *The determinant of a* (m,n) *pretzel is* $|m+n|$ *for any* $m,n\neq0$.

One ought to be able to label the knot in the more general case using a similar scheme to the one we suggested. The computation of the determinant should carry through similarly.

CONJECTURE 5.2. *A* (m,n) *pretzel is a link when both* m *and* n *are even or both are odd. Otherwise the pretzel is a knot.*

PROBLEM 5.3. *What is the determinant of a general* $(m_1,m_2,\cdots,m_k)$ *pretzel?*

REFERENCES

[1] C. LIVINGSTON, "Knot Theory," Mathematical Association of America, Washington, DC, 1993.

Nitish Dass, Jonathan McGrath and Erin Urbanski, St. Olaf College, Northfield, MN 55057.

Nittish Dass, from Kuwait, is currently a senior majoring in mathematics and economics.

John McGrath, from Colorado, is currently a senior mathematics major.

Erin Urbanski, from Minnesota, graduated in May 2000.

The project began in a knot theory course taught by Prof. Dietz at St. Olaf college during the interim term of 1999.

From the Right Side

Overheard in a Bar.

So, who was that woman you were talking to?
Sorry... That's my ex, up to no good.
Oh, I don't mind.
Hey! I trade on the floor. What do you do?
I work in derivatives.
What a start! I feel like we're in the same business.
Not a chance.
I can't see the difference.
It's easy to differentiate!
That's pretty nice.
Absolutely not! Things change all the time.
So, what would you like?
A little continuity.
Perhaps something constant?
Every time I think I've found a constant, it vanishes.
That's rough.
I know, and I just can't operate if things aren't smooth.
Think you'll ever make it to the top?
Why try? It just vanishes too.
And if I grasp what you're telling me, so does the bottom.
Precisely.
But what happens then?
Who knows? I'm at my limit.
Which one?
Top and bottom.
How does that make you feel?
I rate.
Have you ever thought about changing?
Constantly. I wish I could. But how?
Just undo it all.
But how I constantly wish I could.
Have you ever felt that making a change rates just a thought?
But I'm at my limit.
Which one?
Left and right.
But what happens in between?
Who knows? I'm telling you that's precisely why I can't grasp it all.
Why not try to operate more smoothly?
It's still too rough.
Don't think of things as constants...
Now what have you found?
They're vanishing!
Perhaps you can do this every time.
That pretty nicely sums it up.
So, do you like having a little continuity?
Absolutely!
Can you see the difference now?
It's easy to integrate!
You're back where you started?
I feel like there's a chance I'm done with this business.
I'm floored... Hey! What did he just do?
Oh, I should go up, if you don't mind, and give that man a talking to.
Why don't you?
Sorry. It would do no good
Why not? You can differentiate. You can integrate. Why wouldn't it?
That's my e^x.

- Philip Beaver, United States Military Academy

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

ΠΜΕ Journal, Vol. 11, No. 3, pp 139–142, 2000.

THE SEARCH FOR TRI-OPERATE FIELDS

BRETT ALAN ENGE*

1. Introduction. In a first year abstract algebra course one learns about finite and infinite fields and some of their basic properties such as the characteristic of the field. The interest of this research lies in the search for fields whose multiplicative group with some new binary operation star $(*)$ forms a new field. A field whose multiplicative group exhibits this property is called a tri-operate field.

DEFINITION 1.1. *A* tri-operate field is a field such that the non-zero multiplicative structure, $F^\times = F \sim \{0\}$, forms the additive structure of a new field with some new binary operation $*$. That is, $(F, +, \times)$ is a field and $(F^\times, \times, *)$ is a field.

Analyzing the relationship between multiplication and addition provides some insight into how the new binary operation must relate to multiplication. The definition below expresses this relationship.

DEFINITION 1.2. *Let* $n \in Z^+$. *For any* $a \in F$ *define* $n \cdot a \equiv \underbrace{a + a + \cdots + a}_{n \text{ times}} \equiv na$.

$$0 \cdot a \equiv 0. \text{ if } n \in Z \text{ and } n < 0, n \cdot a \equiv |n| \cdot (-a) \equiv na.$$

Since $\times$ *is distributive over* $+$ *for any* $n, m \in Z$ *and* $a \in F$ *it follows that* $(n \cdot a) \times (m \cdot a) = (nm \cdot a) \times a$. *In particular,* $(n \cdot 1) \times a = na$ *where* 1 *is the identity of the field* $(F, +, \times)$.

DEFINITION 1.3. *Let* $n \in Z^+$. *For any* $a \in F$ *define* $n \bullet a \equiv \underbrace{a \times a \times \cdots \times a}_{n \text{times}} \equiv a^n$.

$$0 \bullet a \equiv 1. \text{ If } n \in Z \text{ and } n < 0, n \bullet a \equiv |n| \bullet (a^{-1}) \equiv a^n.$$

Since $*$ *is distributive over* $\times$ *for any* $n, m \in Z$ *and* $a \in F$ *it follows that* $(n \bullet a) * (m \bullet a) = (nm \bullet a) * a = (a^{nm}) * a$. *In particular,* $(n \bullet \epsilon) * a = a^n$ *where* ϵ *is the identity of the field* $(F^\times, \times, *)$.

Before moving on to some general tri-operate field theory we will first look at an example of a tri-operate field to show that they do in fact exist and to better acquaint the reader with what it is we are trying to characterize. We will look at the field $(Z_3, +, \times)$ and its additive and multiplicative structures.

The following table is the group table for $(Z_3, +)$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

*James Madison University

The next table is the group table for $(Z_3^\times, \times)$:

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

We will now look at the group table for $(Z_2, +)$ to observe that $(Z_3^\times, \times) \cong (Z_2, +)$:

+	0	1
0	0	1
1	1	0

Now we can use the definition of Dot to create $(Z_3^*, *)$:

*	1	2
1	1	1
2	1	2

Looking at the table below for $(Z_2^\times, \times)$ shows that $(Z_3^*, *) \cong (Z_2^\times, \times)$:

x	1
1	1

Since $(Z_3^\times, \times) \cong (Z_2, +)$ and $(Z_3^*, *) \cong (Z_2^\times, \times)$ we get that $(Z_3^\times, \times, *) \cong (Z_2, +, \times)$ and therefore $(Z_3^\times, \times, *)$ is a field so $(Z_3, +, \times, *)$ is a tri-operate field.

Now that it is better understood what a tri-operate field is and what one actually looks like we look at some general theorems.

2. General Tri-Operate Field Theory. We note that any trioperate field must have at least three elements because the identities with respect to the three operations are necessarily distinct.

Analyzing the properties of a field and that of dot gives rise to a general lemma that later becomes very important.

LEMMA 2.1. *Let $(F, +, \times)$ be a field. If there exists an element $t \in F, t \neq 0$ such that $p \cdot t = 0, p$ a fixed integer, then for all $x \in F$, $p \cdot x = 0$.*

Proof. Let $t \in F, t \neq 0$, such that $p \cdot t = 0$ and p is a fixed integer. We can write $p \cdot t$ as $0 = p \cdot t = (p \cdot 1) \times t$. Since F is a field either $p \cdot 1 = 0$ or $t = 0$. Since $t \neq 0$, $p \cdot 1 = 0$. □

A special case of the above lemma turns out to be vital to the discovery of what the characteristic, $CharF$, of a field F must be in order for that field to be tri-operate. This special case is:

LEMMA 2.2. *If zero and some $t \neq 0 \in (F, +, \times)$, a field, are their own additive inverses in $(F, +, \times)$ then Char $F = 2$.*

Proof. Since t its own additive inverse, $t+t = 0$, i.e. $2 \cdot t = 0$. Therefore $CharF = 2$ by Lemma 1. □

By exploiting the previous result we obtain our first theorem about the characteristic of a tri-operate field.

THEOREM 2.3. *Let $(F, +, \times, *)$ be a tri-operate field, then Char $F \neq 2$ if and only if Char $F^\times = 2$.*

Proof. ($\Rightarrow$) Suppose Char $F \neq 2$, then -1 and 1 are their own multiplicative inverses in $(F^\times, \times, *)$. By Lemma 2, Char $F^\times = 2$.

($\Leftarrow$) Since $(F, +, \times, *)$ is tri-operate, $|F| > 2$ so $F \supseteq \{0, 1, x\}$ where $0, 1$ and x are all different. Suppose Char $F^\times = 2$ and Char $F = 2$. Since Char $F^\times = 2$, then $\forall y \neq 0, y \in F^\times$, we have $y^2 = 1$. It now follows that $1 = (1 + x)^2 = 1 + 2x + x^2 = 1 + 2x + 1 = 2 + 2x = 0$ which is a contradiction. So Char $F^\times$ and Char F cannot both equal 2. □

For the rest of this section of the paper we will assume that $(F, +, \times, *)$ is a tri-operate field.

The characteristic of $(F^\times, \times, *)$ is either 2 or it is not 2. We will first look at the case where Char $F^\times = 2$.

LEMMA 2.4. *If Char $F^\times = 2$, then the characteristic of $(F, +, \times)$ must be 3.*

Proof. Since Char $F^\times = 2$, by Theorem 1 Char $F \neq 2$ and therefore we know that $\langle -1 \rangle$, the multiplicative group generated by -1, has order 2 in $F^\times$. So in F, {1,-1} is a subgroup of $F^\times$ in F. We will show that $(\langle 1 \rangle, +)$ has order 3 by showing $3 \cdot 1 = 0$.

We know that if $x \in F^\times, x^2 = 1$. Since Char $F \neq 2$, we know $2 \in F$, $2 \neq 0$, so $2 \in F^\times$ and $(2)(2) = 1$.

We can write $4 \cdot 1$ as $1 + 1 + 1 + 1$. So $4 \cdot 1 = 1 + 1 + 1 + 1$ and therefore $(4 \cdot 1)(2) = (1 + 1 + 1 + 1)(2) = (2 + 2)(2) = (2)(2) + (2)(2) = 1 + 1 = 2$, which gives us that $2 + 2 + 2 + 2 = 2$ and $0 = 2 + 2 + 2 = 2(1 + 1 + 1) = 2(3 \cdot 1)$. Since $2 \neq 0$, $3 \cdot 1 = 0$ and it follows that Char $F = 3$. □

Now we know that if a tri-operate field exists it must have characteristic 2, where the exponent of the multiplicative group is not two or it must have characteristic 3, where the exponent of the multiplicative group is 2.

We will now examine the case where Char $F = 3$ which gives rise to the following theorem.

THEOREM 2.5. *The only tri-operate field, $(F, +, \times, *)$ where Char $F^\times = 2$ is Z_3.*

Proof. Since Char $F^\times = 2$, $x^2 = 1$, for all $x \in F^\times$, $x \neq 0$. By Lemma 3, Char $F = 3$, so we know $0, 1, 2, \in F$. Let $x \in F$. Suppose $x \neq 0$ then either $(1 + x) = 0$ which implies $x = 2$, or $(1 + x)(1 + x) = 1$. Let $(1 + x)(1 + x) = 1$. We have $1 + 2x + x^2 = 1$, so $1 + 2x + 1 = 1$ since $x \neq 0$, $x^2 = 1$. Thus $2 + 2x = 1$, $2x = 2$, and $x = 1$. It follows that x is either 0, or 1, or 2. □

It is now time to depart from the general case and look specifically at the finite case. We will now use these results to characterize finite tri-operate fields.

3. Characterization of Finite Tri-Operate Fields. We must first give some background information for finite fields. Let $(F, +, \times)$ be a finite field, then $(F, +)$ is the additive group and is abelian. $(F^\times, \times)$ is the multiplicative group and is abelian as well as cyclic (see e.g. [1], p.267).

In the example Z_3 we notice that $Z_3^\times \cong Z_2$. Below is a generalization of this isomorphism fact which proves to be the key to characterizing the finite case.

THEOREM 3.1. *(Existence of Isomorphism) Let F be denoted by $GF(q^n)$, a Galois Field of order q^n, q a prime, and n a positive integer. There exists an isomorphism*

which maps $(Z_p, +)$ *onto* $(GF^\times(q^n), \times)$ *, where* $p = q^n - 1$ *given by* $\phi : Z_p \longrightarrow GF^\times(q^n)$, $\phi(x) = a^x$, *where* a *is a generator of the multiplicative group* $GF^\times(q^n)$.

This isomorphism allows us to define a new binary operation $*$ such that for all a^x, $a^y \in GF^\times(q^n)$, we have $a^x * a^y = a^{x \times y} = a^{xy}$ and $0 * a^y = 0$ for all $y \in Z_p$ and $a^y \in GF^\times(q^n)$.

The following corollary extends the isomorphism to show that $(GF^\times(q^n), *) \cong (Z_{q^n-1}, \times)$.

COROLLARY 3.2. *If* p *is prime, the mapping* ϕ *is also an isomorphism from* $(Z_p, \times)$ *onto* $(GF^\times, *)$.

From section 1 we know that if F is tri-operate it is either $GF(2^n)$ or Z_3.

The following two theorems show what the order and characteristic of a finite field must be in order for that field to be tri-operate and they completely characterize the finite case.

THEOREM 3.3. *(Characterization Theorem): Let* F *be a finite field.* F *is tri-operate if and only if the order of* F *is* q^n *such that* $q^n - 1$ *is prime, where* q *is prime and* $n \in Z^+$.

Proof. ($\Rightarrow$) Suppose F is a tri-operate field. $(F^\times, \times, *)$ is a field with prime characteristic. $(F^\times, \times)$ is cyclic, so the order and therefore the exponent of $(F^\times, \times)$ is $q^n - 1$. $(F^\times, \times)$ is also the additive structure of $(F^\times, \times, *)$ and so the characteristic of $(F^\times, \times, *)$ is $q^n - 1$, which must be prime.

($\Leftarrow$) Suppose $q^n - 1$ is prime. Then there exists an isomorphism from $(Z_{q^n-1}, +, \times)$ onto $(F^\times, \times, *)$, as defined above, and $(F, +, \times, *)$ is a tri-operate field. □

We summarize our findings as follows.

THEOREM 3.4. *(Finite Tri-operate Fields): Let* $(F, +, \times)$ *be a finite field.* F *is tri-operate if and only if* F *is* $GF(2^n)$, *where* $2^n - 1$ *is prime or* F *is* $Z_3, n \in Z^+$.

Note that the previous theorem could have been deduced without section 1 by showing that $q^n - 1$, where q is prime, can only be prime if $q^n = 3$ or $q^n = 2^n$, where $2^n - 1$ is a Mersenne prime.

Attempting to characterize the infinite case, we can show that if an infinite tri-operate field exists, it only contains Z_2, but no other finite subfield. Moreover, it must contain a transcendental extension of Z_2 plus an n^{th} root for every $n \in Z^+$ of all of the elements of the field. At this point the question as to whether or not such a field is tri-operate or if infinite tri-operate fields even exist is still unanswered.

REFERENCES

[1] MCCOY and JANUSZ, *Introduction to Modern Algebra*, Fifth Edition, McGraw-Hill, 1998.

Brett Alan Enge (benge@calvin.math.vt.edu).

Brett Alan Enge was an undergraduate student at James Madison University. This work arose out of a summer research project under the direction of Dr. Carter G. Lyons.

ΠME Journal, Vol. 11, No. 3, pp 143-144, 2000.

CIRCULAR FUNCTIONS OF MULTIPLE INTEGRAL ANGLES

MATTHEW J. HALE*

My desk light kept me company late that Thursday night. Various pre-calculus problems were scattered across my desktop as I leaned over the current assignment. My pencil scribbled furiously as I solved for expressions such as $\cos(8x)$ or $\sin(5x)$ in terms of $\cos(x)$ or $\sin(x)$. As I waded through the intricacies of the problem, I couldn't help but wonder; isn't there a simpler way to solve trigonometric functions of integral angles?

As it turned out, my curiosity got the best of me. Failing to discover any theorem which allowed trigonometric functions of integral values to be easily solved, I set out to develop such a theorem on my own. The result of my enquiry is the subject of this paper.

Let us return to our example of $\cos(8x)$. Using the trigonometric double angle identities [1], pp. 428-429, we are able to simplify $\cos(8x)$ conventionally, using algebraic operations.

$$\begin{aligned}\cos(8x) &= \cos^2(4x) - \sin^2(4x)\\ &= [\cos^2(2x) - \sin^2(2x)]^2 - [2\sin(2x)\cos(2x)]^2\\ &= \{[\cos^2(x) - \sin^2(x)]^2 - [2\sin(x)\cos(x)]^2\}^2\\ &\quad -\{2[2\sin(x)\cos(x)][\cos^2(x) - \sin^2(x)]\}^2\\ &= \cos^8(x) - 28\sin^2(x)\cos^6(x) + 70\sin^4(x)\cos^4(x)\\ &\quad -28\sin^6(x)\cos^2(x) + \sin^8(x)\end{aligned}$$

Our other example, $\sin(5x)$, is similar. After expansion, we obtain:

$$\sin(5x) = 5\cos^4(x)\sin(x) - 10\cos^2(x)\sin^3(x) + \sin^5(x)$$

Whether the integral angle being solved for is odd or even, the trigonometric addition identities [1], pp. 416-422, may be used in expansion. (The double angle identities are, after all, a special case of the addition identities.) However, there is a simpler method. Recall De Moivre's Theorem [1], pp. 498-501, taught in many high school pre-calculus or calculus courses. With little effort, this theorem yields a more practical method of simplifying circular functions of integral angles.

By De Moivre's Theorem,

$$\cos(nx) + i\sin(nx) = (\cos(x) + i\sin(x))^n$$

Elaboration of the right side by the Binomial Theorem yields:

$$\cos(nx) + i\sin(nx) = (\cos(x) + i\sin(x))^n = \sum_{k=0}^{n} \binom{n}{k} \cos^{n-k}(x) i^k \sin^k(x)$$

So

$$\cos(nx) = \sum_{k=0}^{n} (-1)^k \binom{n}{2k} \cos^{(n-2k)}(x) \sin^{2k}(x)$$

*St. Xavier High School

with the understanding that $\binom{n}{2k} = 0$ for $2k > n$. Similarly,

$$\sin(nx) = \sum_{k=0}^{n} (-1)^k \binom{n}{2k-1} \cos^{(n-2k-1)}(x) \sin^{(2k+1)}(x).$$

Now a trig problem such as $\cos(8x)$ is easily done:

$$\begin{aligned}\cos(8x) &= \sum_{k=0}^{4} (-1)^k \binom{8}{2k} \cos^{(8-2k)}(x) \sin^{(2k)}(x) \\ &= \cos^8(x)\sin^0(x) - 28\cos^6(x)\sin^2(x) + 70\cos^4(x)\sin^4(x) \\ &\quad -28\cos^2(x)\sin^6(x) + \cos^0(x)\sin^8(x).\end{aligned}$$

Try $\sin(5x)$ on your own.

We are now able to solve $\cos(nx)$ or $\sin(nx)$ in terms of $\cos(x)$ and $\sin(x)$ for every natural number n. Since cosine is an even function and sine is an odd function, we can easily extend the equations to the case that n is an integer.

What if n is rational or real? De Moivre's Theorem is usually proven by induction [1], p. 498, from which we can guarantee that it holds true only for the natural numbers. However, it is possible to extend De Moivre's Theorem to the rational numbers, and so there is some hope of generalizing the sigma notation equations when n is rational. On the other hand, if n is not rational, De Moivre's Theorem leads to nonsense, such as the result in [2].

REFERENCES

[1] MARY P. DOLCIANI, et. al, "Modern Introductory Analysis," Houghton Mifflin Company, Boston, MA, 1977.

[2] PETER M. JARVIS, *Fourier Analysis is Trivial,* The College Mathematics Journal, 31, No. 3, 207–208, 2000.

Matthew J. Hale, St. Xavier High School, Norwood, OH.

Reviewer's Note: Even though this result seems obvious to anyone who has taken a course in Complex Analysis using the definitions of $\mathrm{Re}(e^{iz})$ and $\mathrm{Im}(e^{iz})$, textual references to the method are quite sparse. Marsden, "Basic Complex Analysis", Freeman, 1973, p. 40, says that all trigonometric identities can be deduced in this way. Levinson & Redhoffer, "Complex Variables", Holden Day, 1970 discusses the issue in his section on harmonic functions and gives some examples in his exercises. Nehari, "Complex Variables", Allyn and Bacon, 1961 also uses the method to evaluate some trigonometric series. But the reviewer could find this beautiful relationship nowhere in a dozen or more textbooks. That fact makes this discovery by a student still in high school even more meaningful. Dr. Dipendra Bhattacharya, however, noted that the result in question is found in Loney's "Complex Variables", part 2, p. 32 published in New Delhi by S. Chand & Co. in 1893 (reprinted in 1988).

Stephen Gendler, Clarion University.

ΠME Journal, Vol. 11, No. 3, pp 145–148, 2000.

AN ITERATIVE ALGORITHM FOR SOLVING QUADRATIC EQUATIONS

S. A. KHURI*

1. Introduction. "Completing the square" on the quadratic equation

$$ax^2 + bx + c = 0 \tag{1.1}$$

leads to the quadratic formula,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{1.2}$$

where a, b, and c are real numbers with $a \neq 0$.

Lindstrom [1] presented alternative ways for deriving the quadratic formula based on assuming the solutions to be complex numbers expressed in both trigonometric and rectangular forms. In this paper, we present an iterative technique for deriving the quadratic formula.

2. Applying the iterative method. The method consists of representing the solution of (1.1) as an infinite series of the form

$$x = x_0 + x_1 + x_2 + x_3 + \ldots = \sum_{n=0}^{\infty} x_n \tag{2.1}$$

To solve the quadratic equation (1.1), we first rewrite it as

$$x = \alpha + \beta x^2 \tag{2.2}$$

where

$$\alpha = -\frac{c}{b}, \quad \beta = -\frac{a}{b} \tag{2.3}$$

Upon substituting the solution given in (2.1) into the quadratic equation (2.2) yields

$$\begin{aligned}\textstyle\sum_{n=0}^{\infty} x_n &= x_0 + x_1 + x_2 + x_3 + \ldots \\ &= \alpha + \beta\left(x_0 + x_1 + x_2 + x_3 + \ldots\right)^2 \\ &= \alpha + \beta\left[x_0^2 + 2x_0x_1 + x_1^2 + 2x_1x_2 + 2x_0x_3 + 2x_0x_4 + 2x_1x_3 + x_2^2 + \ldots\right]\end{aligned} \tag{2.4}$$

Upon matching both sides of equation (2.4), results in the following iterative algorithm,

$$\begin{cases} x_0 = \alpha \\ x_1 = \beta x_0^2 \\ x_2 = \beta\left(2x_0x_1\right) \\ x_3 = \beta\left(x_1^2 + 2x_0x_2\right) \\ x_4 = \beta\left(2x_0x_3 + 2x_1x_2\right) \\ x_5 = \beta\left(2x_0x_4 + 2x_1x_3 + x_2^2\right) \\ \ldots \end{cases} \tag{2.5}$$

*American University of Sharjah, UAE

Solving equations (2.5) iteratively we get,

$$(2.6)\quad \begin{cases} x_0 = \alpha \\ x_1 = \beta x_0^2 = \beta\alpha^2 \\ x_2 = \beta\left(2x_0x_1\right) = \beta\left[2\alpha\left(\alpha^2\beta\right)\right] = 2\beta^2\alpha^3 \\ x_3 = \beta\left(x_1^2 + 2x_0x_2\right) = \beta\left[\beta^2\alpha^4 + 2\alpha\left(2\beta^2\alpha^3\right)\right] = 5\beta^3\alpha^4 \\ x_4 = \beta\left(2x_0x_3 + 2x_1x_2\right) = \beta\left[2\alpha\left(5\beta^3\alpha^4\right) + 2\alpha^2\beta\left(2\beta^2\alpha^3\right)\right] = 14\beta^4\alpha^5 \\ \ldots \end{cases}$$

Thus the infinite series solution of the quadratic equation is given by:

$$(2.7)\quad \begin{aligned} x &= x_0 + x_1 + x_2 + x_3 + \ldots \\ &= \alpha + \beta\alpha^2 + 2\beta^2\alpha^3 + 5\beta^3\alpha^4 + 14\beta^4\alpha^5 + \ldots \\ &= \tfrac{1}{2\beta}\left[2\alpha\beta + 2(\alpha\beta)^2 + 4(\alpha\beta)^3 + 10(\alpha\beta)^4 + 28(\alpha\beta)^5 + \ldots\right] \\ &= \tfrac{1}{2\beta}\left[1 - 1 + 2\alpha\beta + 2(\alpha\beta)^2 + 4(\alpha\beta)^3 + 10(\alpha\beta)^4 + 28(\alpha\beta)^5 + \ldots\right] \\ &= \tfrac{1}{2\beta} - \tfrac{1}{2\beta}\left[1 - 2\alpha\beta - 2(\alpha\beta)^2 - 4(\alpha\beta)^3 - 10(\alpha\beta)^4 - 28(\alpha\beta)^5 - \ldots\right] \\ &= \tfrac{1}{2\beta} - \tfrac{1}{2\beta}\sqrt{1 - 4(\alpha\beta)} \end{aligned}$$

where in the last step of equation (2.7) we used the Maclaurin series expansion of the function $\sqrt{1-4x}$ which is given by

$$(2.8)\quad \begin{aligned} \sqrt{1-4x} &= 1 - 2x - \textstyle\sum_{n=2}^{\infty} 1.3.5\ldots(2n-3)\frac{2^n}{n!}x^n \\ &= 1 - 2x - 2x^2 - 4x^3 - 10x^4 - 28x^5 - \ldots \end{aligned}$$

The Maclaurin expansion in (2.8) converges for

$$|4x| = |4\alpha\beta| = 4\left|\frac{-c}{b}\frac{-a}{b}\right| = \frac{4|ac|}{b^2} < 1$$

which implies that the technique converges if

$$(2.9)\qquad b^2 - 4|ac| > 0$$

For $ab > 0$, condition (2.9) states that the descriminant is positive, which therefore implies that for real roots the method converges. A divergence series may indicate repeated roots, complex roots or real roots with $ac < 0$.
Upon substituting the values of $\alpha = -\frac{c}{b}$, $\beta = -\frac{a}{b}$ given in equation (2.3), the solution in (2.6) becomes:

$$(2.10)\quad \begin{aligned} x &= \tfrac{1}{2\beta} - \tfrac{1}{2\beta}\sqrt{1 - 4(\alpha\beta)} \;\; = \tfrac{-b}{2a} + \tfrac{b}{2a}\sqrt{1 - 4\tfrac{ac}{b^2}} \\ &= -\tfrac{b}{2a} + \tfrac{b}{2a|b|}\sqrt{b^2 - 4ac} \end{aligned}$$

The next two cases follow from the solution given in equation (2.10).
Case 1: If $b > 0$ then the solution in (2.10) becomes:

$$(2.11)\qquad x = \frac{-b+\sqrt{b^2-4ac}}{2a}$$

Therefore, the scheme converges to only one root, as for the second solution it can be obtained and approximated by factoring. Note that the solution (2.11) implies that:
• If $b > 0$ and $a > 0$ then the method converges to the larger solution.

• If $b > 0$ and $a < 0$ then the method converges to the smaller solution.
Case 2: If $b < 0$ then from equation (2.10) the technique converges to the solution:

$$(2.12)\qquad x = \frac{-b-\sqrt{b^2-4ac}}{2a}$$

As for the second solution, it can be approximated by factoring the quadratic equation. The solution in (2.12) results in the following two conditions:
• If $b < 0$ and $a > 0$ then the method converges to the smaller solution.
• If $b < 0$ and $a < 0$ then the method converges to the larger solution.

3. Examples. In this section, the algorithm described in the previous section is applied to some examples of the quadratic equation. For convenience, in the next numerical computations let the expression

$$(3.1)\qquad S_n = \sum_{i=0}^{n} x_i$$

denote the n-th term approximation to the solution x, where x_i's are the iterates.

EXAMPLE 1. Consider the equation

$$(3.2)\qquad -x^2 - 18x + 40 = 0$$

whose solutions are $x = -20$ and $x = 2$. For this case,

$$a = -1, \quad b = -18 \quad \text{and} \quad c = 40$$

The scheme (2.6) and equation (2.3) give the following iterates and partial sums of the approximate solution:

$$(3.3)\quad \begin{aligned} x_0 &= 2.2222222222 \\ x_1 &= -0.2743484225 \\ x_2 &= 0.06774035123 \\ x_3 &= -0.02090751581 \\ x_4 &= 0.00722728942 \\ x_5 &= -0.00267677386 \end{aligned}$$

$$(3.4)\quad \begin{aligned} S_1 &= 1.947873800 \\ S_2 &= 2.015614151 \\ S_3 &= 1.994706635 \\ S_4 &= 2.001933925 \\ S_5 &= 1.999257151 \end{aligned}$$

According to our previous analysis, for the case where $b < 0$ and $a < 0$ the technique converges indeed to the larger solution which is $x = 2$.

EXAMPLE 2. Consider the equation

$$(3.5)\qquad -x^2 + 9x + 10 = 0$$

whose solutions are $x = -1$ and $x = 10$. As before, our scheme yields:

$$\begin{aligned} x_0 &= -1.1111111111 \\ x_1 &= 0.1371742112 \\ x_2 &= -0.0338701756 \\ x_3 &= 0.0104537579 \\ x_4 &= -0.0036136447 \\ x_5 &= 0.0013383869 \end{aligned} \tag{3.6}$$

$$\begin{aligned} S_1 &= -0.973936899 \\ S_2 &= -1.007807075 \\ S_3 &= -0.997353318 \\ S_4 &= -1.000966962 \\ S_5 &= -0.999628575 \end{aligned} \tag{3.7}$$

Clearly the scheme converges to the smaller root which is $x = -1$. By our previous analysis, this is justified by the fact that for this example $a < 0$ and $b > 0$.

EXAMPLE 3. Consider the equation

$$2x^2 + 203x + 300 = 0 \tag{3.8}$$

whose solutions are $x = -100$ and $x = -1.5$. For this case we get:

$$\begin{aligned} x_0 &= -1.477832512 \\ x_1 &= -0.021517132 \\ x_2 &= -0.000626576 \\ x_3 &= -0.000022807 \\ x_4 &= -0.000000930 \\ x_5 &= -0.000000041 \end{aligned} \tag{3.9}$$

$$\begin{aligned} S_1 &= -1.499349645 \\ S_2 &= -1.499976220 \\ S_3 &= -1.499999028 \\ S_4 &= -1.499999957 \\ S_5 &= -1.499999998 \end{aligned} \tag{3.10}$$

Since $a > 0$ and $b > 0$ the method, according to the previous analysis, converges to the larger solution which is $x = -1.5$.

These examples show that our scheme converges very fast and only few iterates are needed to obtain an error of less than 1%. Observe, moreover, that the farther apart the two solutions are, the faster the scheme converges to the exact solution.

REFERENCES

[1] PETER A. LINDSTROM, *The quadratic formula revisited again,* Pi Mu Epsilon Journal 10 (6), 461-463 (1997).

S. A. Khuri, Department of Computer Science, Mathematics and Statistics, American University of Sharjah, P.O.Box 26666, Sharjah-U.A.E., Fax: 971-6-5585066.

ΠME Journal, Vol. 11, No. 3, pp 149–152, 2000.

A GENERALIZATION OF THE HATCHECK PROBLEM*

PAUL KLINGSBERG AND GINA M. PANICHELLA

Abstract. We investigate the question: How many permutations of n letters contain no k–cycle?

1. Introduction. The problem we have generalized, familiar to all students of combinatorics, is the so–called

> **Hatcheck Problem.** *Suppose that each of n people checked a hat as he/she entered a theater to watch a play. If, at the end of the play, the person in charge of the checked hats distributes the hats at random, giving each of the n people one randomly selected hat, what is the probability that no one receives his or her own hat back?*

Less colorfully but more precisely stated: Let S_n denote the group of all $n!$ permutations of the set $\{1, \ldots, n\}$. If you choose an element of S_n uniformly at random (*i.e.*, so that each permutation has probability $1/n!$ of being chosen), what is the probability P_n that the permutation you choose will have no fixed points? It turns out (see [1], §6.3) that

$$P_n = \frac{1}{n!}\sum_{t=0}^{n}\frac{(-1)^t n!}{t!} = \sum_{t=0}^{n}\frac{(-1)^t}{t!}, \tag{1}$$

so that asymptotically, the probability is

$$\lim_{n\to\infty} P_n = \lim_{n\to\infty}\left(\sum_{t=0}^{n}\frac{(-1)^t}{t!}\right) = \sum_{t=0}^{\infty}\frac{(-1)^t}{t!} = e^{-1}. \tag{2}$$

To see how to generalize this problem, recall that every element of S_n admits a unique *disjoint cycle factorization* (*DCF*)—see [3], Ch. 5, for details. For each $1 \le k \le n$, we define

$$P_{n,k} := \text{ The fraction of elements in } S_n \text{ whose DCFs contains no } k\text{–cycles.}$$

Of course, $P_{n,1}$ is just P_n; but we could equally well ask for $P_{n,2}$, the proportion of elements of S_n whose DCF's contain no 2–cycles. (In hatcheck terms, this is the probability that no two people receive each other's hats.) It is this more general question that we address here.

> **Generalized Hatcheck Problem.** *For any $1 \le k \le n$, what is the value of $P_{n,k}$? What is $\lim_{n\to\infty} P_{n,k}$?*

2. The Principle of Inclusion–Exclusion. In introductory combinatorics, the Hatcheck Problem is solved by applying to it the so-called *Principle of Inclusion–Exclusion* (or *PIE*), and this is also the tool we use to solve the generalized problem. We state here the version of the PIE we will need; the interested reader will find a proof in any introductory combinatorics text, for example [1]. We begin with a finite set Ω of *objects* and a finite set P of *properties*, and we suppose that each object either does or does not *possess* each property; in other words, we are supposing that to each object $\omega \in \Omega$, we have an associated set $\text{prop}(\omega) \subseteq P$ of properties that ω possesses. (In the case of the Hatcheck Problem, one takes Ω to be S_n; and, for

*St. Joseph's University

each $1 \le i \le n$, one takes property i to be that of having i as a fixed point. Thus for any element $\sigma \in S_n$, $\text{prop}(\sigma)$ is the set of fixed points of σ.) Next, for each subset $S \subseteq P$, we put

$$N_{\ge}(S) := |\{\omega \in \Omega : \text{prop}(\omega) \supseteq S\}|$$

and

$$N_{=}(S) := |\{\omega \in \Omega : \text{prop}(\omega) = S\}|$$

(where we use $|T|$ to denote the number of elements in a finite set T). The PIE, then, is the rule that prescribes how to compute the numbers $\{N_{=}(S)\}$ from the numbers $\{N_{\ge}(S)\}$. We need here only the formula for $N_{=}(\emptyset)$, the number of objects that possess no properties whatever:

$$N_{=}(\emptyset) = \sum_{S \subseteq P} (-1)^{|S|} N_{\ge}(S). \tag{3}$$

3. Applying the PIE to the Generalized Problem. Fix $k \ge 1$. As in the case of the Hatcheck Problem, we take Ω to be S_n. P will be the set of all possible k–cycles in S_n; there are $\binom{n}{k}(k-1)!$ of these. For $\sigma \in S_n$ and $\mathcal{C} \in P$, we will say that σ *possesses property* $\mathcal{C}$ iff σ contains $\mathcal{C}$ in its DCF. Thus, the numerator of $P_{n,k}$—the number of elements $\sigma \in S_n$ such that the DCF of σ contains no k–cycle—will be $N_{=}(\emptyset)$. We cannot use formula (3) to compute it, however, until we have found the numbers $N_{\ge}(S)$. This is the content of Theorem 1.

THEOREM 1. *Let S be a set of k–cycles in S_n.*

(a) If S contains two different k–cycles that have one or more integers in common then $N_{\ge}(S) = 0$.

(b) Otherwise, if the k–cycles in S are pairwise disjoint, $N_{\ge}(S) = (n - k|S|)!$.

Proof. (a) If $\mathcal{C}_1 \ne \mathcal{C}_2 \in S$ are nondisjoint, then $\mathcal{C}_1$ and $\mathcal{C}_2$ are inconsistent with each other and so cannot both appear in the DCF of any permutation σ.

(b) Let $S = \{\mathcal{C}_1, \ldots, \mathcal{C}_t\}$ consist of t pairwise-disjoint k–cycles. (Note that these t k–cycles involve kt different integers, so that necessarily $t \le \lfloor n/k \rfloor$.) A permutation $\sigma \in S_n$ will include all of $\mathcal{C}_1, \ldots, \mathcal{C}_t$ in its DCF iff σ permutes the kt integers that appear in these cycles exactly as the cycles do; σ may permute the remaining $(n - kt)$ integers among themselves in any fashion. Clearly, there are exactly $(n - kt)!$ such permutations σ. □

We now combine Theorem 1 with some standard counting arguments to obtain a simple formula for $N_{=}(\emptyset)$.

THEOREM 2. *The number of elements $\sigma \in S_n$ such that the DCF of σ contains no k–cycles is given by the expression*

$$\sum_{t=0}^{\lfloor n/k \rfloor} \frac{\left(-\frac{1}{k}\right)^t n!}{t!}.$$

Proof. By the PIE, as already noted, we have that the number of such $\sigma \in S_n$ is

$$N_{=}(\emptyset) = \sum_{S \subseteq P} (-1)^{|S|} N_{\ge}(S).$$

By Theorem 1, we can restrict this sum to subsets $S' \subseteq P$ such that the k–cycles in S' are pairwise disjoint, in which case $N_{\ge}(S') = (n - k|S'|)!$. This gives

$$N_{=}(\emptyset) = \sum_{S' \subseteq P} (-1)^{|S'|} (n - k|S'|)!. \tag{4}$$

Now, the summands in equation (4) depend only on the sizes of the sets $\{S'\}$, so we can gather terms by cardinality $t = |S'|$:

$$N_{=}(\emptyset) = \sum_{t=0}^{\lfloor n/k \rfloor} \underbrace{\begin{pmatrix} \text{number of sets } S' \subseteq P \text{ such that } S' \\ \text{contains } t \text{ pairwise-disjoint } k\text{–cycles} \end{pmatrix}}_{(*)} \cdot (-1)^t (n - kt)!. \tag{5}$$

The next question is: What does $(*)$ equal in equation (5)? In other words: For $0 \le t \le \lfloor n/k \rfloor$, in how many ways is it possible to choose a set of t pairwise-disjoint k–cycles from S_n? The answer to this question is well-known (it appears in [2], for example), but for completeness, we outline the method of solution here. The number of such sets of k–cycles is equal to the number of ways of doing all of the following.

Step:	**Number of Ways:**
1. Choose kt integers from $\{1, \ldots, n\}$.	$\binom{n}{kt}$ ways
2. Partition these kt integers into t subsets of k elements each.	$(kt)!/(t!(k!)^t)$ ways
3. Arrange each of the t k–element sets from Step 2 into a k–cycle.	$((k-1)!)^t$ ways

Thus, in equation (5), quantity $(*)$ equals the product of the expressions in the "Number of Ways" column:

$$(*) = \binom{n}{kt} \cdot \frac{(kt)!}{t!(k!)^t} \cdot ((k-1)!)^t = \frac{n!}{t!k^t(n-kt)!}. \tag{6}$$

Finally, substituting expression (6) into equation (5) and simplifying gives

$$N_{=}(\emptyset) = \sum_{t=0}^{\lfloor n/k \rfloor} \underbrace{\frac{n!}{t!k^t(n-kt)!}}_{(*)} \cdot (-1)^t (n-kt)! = \sum_{t=0}^{\lfloor n/k \rfloor} \frac{\left(-\frac{1}{k}\right)^t n!}{t!}.$$

□

As an immediate consequence, we are able to solve the Generalized Hatcheck Problem with formulas that generalize (1) and (2), namely

$$P_{n,k} = \sum_{t=0}^{\lfloor n/k \rfloor} \frac{\left(-\frac{1}{k}\right)^t}{t!} \quad \text{and} \quad \lim_{n \to \infty} P_{n,k} = e^{-1/k}.$$

4. An extension. The natural question to consider next is the number of permutations that avoid more than one type of cycle in their DCFs. For example, let P_{n,k_1,k_2} $(1 \le k_1 < k_2)$ denote the probability that a randomly chosen element $\sigma \in S_n$ contains no k_1–cycles and no k_2–cycles; in hatcheck terms, $P_{n,1,2}$ is the probablity that no one receives his or her own hat and that no two people receive each other's hats. It

turns out that *asymptotically*, such probabilities are mutually independent—not only pairwise but also in larger sets. Thus (for the example)

$$\lim_{n\to\infty} P_{n,k_1,k_2} = e^{-\left(\frac{1}{k_1}+\frac{1}{k_2}\right)} = \left(\lim_{n\to\infty} P_{n,k_1}\right)\left(\lim_{n\to\infty} P_{n,k_2}\right)$$

so that

$$\lim_{n\to\infty} P_{n,1,2} = e^{-\frac{3}{2}}.$$

The details will be set out in a future paper.

REFERENCES

[1] BRUALDI, RICHARD A., "Introductory Combinatorics", third edition, Prentice Hall, 1999.
[2] DEBRUIJN, N.G., *Pólya's theory of counting*, in Edwin Beckinbach (ed), "Applied Combinatorial Mathematics", John Wiley & Sons, 1964.
[3] GALLIAN, JOSEPH A., "Contemporary Abstract Algebra", fourth edition, Houghton Mifflin Company, 1998.

Paul Klingsberg and Gina M. Panichella, St. Joseph's University, 5600 City Ave., Philadelphia PA 19131

Paul Klingsberg earned his Ph.D. in mathematics from the University of Pennsylvania in 1977. He has been at St. Joseph's University since 1981.

Gina M. Panichella will be a senior majoring in mathematics at St. Joseph's University. She has been a member of ΠΜΕ since the end of her sophomore year.

Call for Referees. Every article in this journal is refereed by a dedicated mathematician. If you are willing to serve as a referee, please email your name, affiliation, mailing address, and those mathematical specialities you feel competent to referee to bservat@wpi.edu (Brigitte Servatius).

ΠME Journal, Vol. 11, No. 3, pp 153–167, 2000.

PROBLEM DEPARTMENT

EDITED BY 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 communications should be addressed to C. W. Dodge, 5752 Neville/Math, University of Maine, Orono, ME 04469-5752. **Please note my new e-mail address: dodge@maine.edu.** *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 July 1, 2001. Solutions identified as by students are given preference.*

Problems for Solution.

994. *Proposed by the editor.*

Although the alphametic $BRENNER = (JOEL)^2$ has no solution in base ten, there is a number M such that $BRENNER$ is the square of a positive integer x in every base greater than or equal to M. Furthermore, the same four digits are used for B, R, E, and N in each such base. Find these digits, the value of M, and the digits of x, the square root of $BRENNER$.

995. *Proposed by Peter A. Lindstrom, Batavia, New York.*

a) Consider the *geometric-arithmetic* recursive sequence f given by

$$f(1) = a, f(2) = ar + d, \text{ and } f(i) = rf(i-1) + d \text{ for } i \geq 2,$$

where a, d, and r are nonzero constants, $r \neq 1$, and i is an integer. Express $\sum_{i=1}^{n} f(i)$ in closed form.

b) Consider the *arithmetic-geometric* recursive sequence g given by

$$g(1) = a, g(2) = r(a + d), \text{ and } g(i) = r(g(i-1) + d) \text{ for } i \geq 2,$$

where a, d, and r are nonzero constants, $r \neq 1$, and i is an integer. Express $\sum_{i=1}^{n} g(i)$ in closed form.

996. *Proposed by Ice B. Risteski, Skopje, Macedonia.*

If $P_i(x)$ is the Legendre polynomial, given by $P_0(x) = 1$ and for positive integral n,

$$P_n(x) = \frac{1}{2^n n!}\frac{d^n}{dx^n}(x^2-1)^n,$$

show that

$$nP_n(\cos x) = \sum_{m=1}^{n} \cos(mx) P_{n-m}(\cos x).$$

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

Evaluate the integral

$$\int_4^8 \frac{\ln(9-x)dx}{\ln(9-x)+\ln(x-3)}.$$

998. *Proposed by David Iny, Baltimore, Maryland.*
For nonnegative integers k and n, let

$$J_{kn} = \frac{1}{(1+k)^2}\binom{n}{0} - \frac{1}{(2+k)^2}\binom{n}{1} + \cdots + \frac{(-1)^n}{(n+k+1)^2}\binom{n}{n}.$$

a) Determine the value of b_k such that the limit L_k exists, where

$$L_k = \lim_{n\to\infty}[(n+1)(n+2)\cdots(n+k+1)J_{kn} - b_k \ln(n+1)].$$

b) Evaluate L_k using your value of b_k and the definition of Euler's constant γ given by

$$\gamma = \lim_{n\to\infty}\left[\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}\right) - \ln n\right] = 0.577\ldots$$

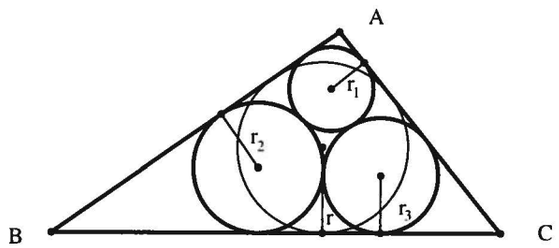
c) Using your results of parts (a) and (b), evaluate, if it exists,

$$\lim_{k\to\infty}\left(\frac{L_k}{k!} + \ln k\right).$$

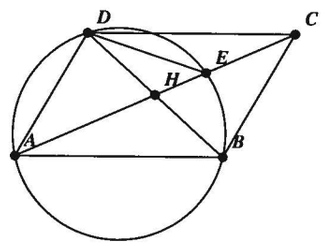
999. *Proposed by the late Jack Garfunkel, Flushing, New York.*
Prove that

$$r \le \frac{(r_1+r_2+r_3)(3+\sqrt{3})}{9},$$

with equality when $r_1 = r_2 = r_3$, where r is the inradius of triangle ABC and r_1, r_2, and r_3 are the radii of the mutually tangent circles in the *Malfatti configuration*, shown in the accompanying figure.



1000. *Proposed by Albert White, St. Bonaventure University, St. Bonaventure, New York.*
Let $ABCD$ be a parallelogram with $\angle A = 60°$. Let the circle through A, B, and D intersect AC again at E and let AC and BD meet at H. See the figure.



Let $[PQR]$ denote the area of triangle PQR. Show that
a) $[DHE]\cdot(AC)^2 = [ADH]\cdot(DB)^2$,
b) $[ADE] - [DEC] = 2[DHE]$, and
c) $2(HE)\cdot(AC) = (DB)^2$.

1001. *Proposed by David Tselnik, Fargo, North Dakota.*
The *Euler numbers* E_n, for $n = 0, 1, 2, \ldots$, are defined by

$$\operatorname{sech} x = \frac{1}{\cosh x} = \sum_{n=0}^{\infty}\frac{E_n}{n!}x^n,$$

so that $E_n = 0$ for all odd n, $E_0 = 1$, $E_2 = -1$, $E_4 = 5$, $E_6 = -61$, etc. Prove the following relations:

a) $\displaystyle\sum_{j=0}^{2m}\binom{4m}{2j}|E_{2j}| = 2\sum_{k=0}^{m}\binom{4m}{4k}E_{4k}$ for $m = 1, 2, 3, \ldots$,

b) $\displaystyle\sum_{j=0}^{2m+1}\binom{4m+2}{2j}|E_{2j}| = 2\sum_{k=0}^{m}\binom{4m+2}{4k}E_{4k}$ for $m = 0, 1, 2, \ldots$,

c) $\displaystyle\sum_{j=0}^{2m}\binom{4m}{2j}|E_{2j}| = -2\sum_{k=1}^{m}\binom{4m}{4k-2}E_{4k-2}$ for $m = 1, 2, 3, \ldots$, and

d) $\displaystyle\sum_{j=0}^{2m+1}\binom{4m+2}{2j}|E_{2j}| = -2\sum_{k=0}^{m}\binom{4m+2}{4k+2}E_{4k+2}$ for $m = 0, 1, 2, \ldots$.

1002. *Proposed by L. Seagull, Glendale Community College, Glendale, Arizona.*
Let n be a composite integer greater than or equal to 48. Prove that between n and $S(n)$ there exist at least five primes, where $S(n)$ is the Smarandache function: for any positive integer n, $k = S(n)$ if k is the smallest positive integer such that n divides $k!$. Then, for example, $S(3) = 3$ and $S(8) = 4$.

1003. *Proposed by I. M. Radu, Bucharest, Romania.*
Show that between $S(n)$ and $S(n+1)$, where $S(n)$ is the Smarandache function, there exists at least one prime number. See Problem 1002 for the definition of the Smarandache function.

1004. *Proposed by Robert C. Gebhardt, Hopatcong, New Jersey.*
Find the minimum value of $f_n = x_1 + x_2 + \cdots + x_n$ if the x_k are all nonnegative and

$$\sum_{k=1}^{n}\cos^2 x_k = 1.$$

1005. *Proposed by Ayoub B. Ayoub, Pennsylvania State University, Abington College, Abington, Pennsylvania.*
Prove that, if $n > 2$ is an odd number,

$$\sum_{k=1}^{(n-1)/2}\sin\frac{4k\pi}{n} = \sin\frac{4\pi}{n} + \sin\frac{8\pi}{n} + \cdots + \sin\frac{2(n-1)\pi}{n} < 0.$$

***1006.** *Proposed by Richard I. Hess, Rancho Palos Verdes, California.*

a) How many aces can be served in one game of tennis?

b) How many consecutive aces can be served in one game of tennis?

c) You and I are playing a set of tennis. In the last 8 points you have served 7 aces and I have served 1. What is our score?

d) In a tennis match you have just served aces on 6 consecutive points. What is the score?

Solutions.

966. [Fall 1999] *Proposed by Count Juan Mower, Big Twenty Township, Maine.*

Although there are several solutions to this base eleven addition alphametic in which 7 divides $SEVEN$ or where 8 divides $EIGHT$, there is only one in which 5 divides $FIVE$. Find that solution:

$$FIVE + SEVEN + EIGHT = TWENTY.$$

Curiously, in that unique solution, 5 divides $EIGHT$, too.

Solution by **Patrick J. Niemczak,** *Alma College, Alma Michigan.*

Immediately, $T = 1$. From the units column we see that we cannot have $E = 10$ or $N = 10$. Also $S \neq 10$ since then we would have $E = W$. From the 11^3 column, $F + I = 10$ or 11. Because it is more plausible to expect a carry from the 11^2 column, we explore $F + I = 10$. There are seven possibilities for F and I, but only $F = 10$ and $I = 0$ avoids difficulties. Since a number in base eleven is divisible by 5 if the sum of its digits is divisible by 5, then $V + E = 10$ or 15. None of the four combinations that produce the sum of 10 will work, and the combination that produces results is $V = 6$ and $E = 9$. Now there must be a 1 carried into the 11 column from the units column, forcing $H = 7$ and 2 is carried into the next column. In the 11^2 column, $2 + 0 + 6 + G = N + 11$. So $G = 5$ or 8. But $G = 5$ requires $N = 2$ and in the units column $Y = 1$, which is not possible. So $G = 8$ and $N = 5$ and $Y = 4$. From the 11^4 column we now have $S = 3$ and $W = 2$. Using t for ten, our solution looks like

$$t069 + 39695 + 90871 = 129514.$$

Also solved by **Charles D. Ashbacher**, Charles Ashbacher Technologies, Hiawatha, IA, **Kenneth B. Davenport**, Frackville, PA, **Mark Evans**, Louisville, KY, **Victor G. Feser**, University of Mary, Bismarck, ND, **Richard I. Hess**, Rancho Palos Verdes, CA, **Rex H. Wu**, Brooklyn, NY, and the **Proposer.**

967. [Fall 1999] *Proposed by Mohammad K. Azarian, University of Evansville, Evansville, Indiana.*

Let N be a natural number greater than 1 with d distinct positive prime divisors. If p and q are the largest and smallest of these divisors, then prove that

$$\log_p N \leq d \leq \log_q N.$$

Solution by **Alma College Problem Solving Group**, *Alma College, Alma, Michigan.*

We take the phrase"Let N be a natural number greater than 1 with d distinct positive prime divisors" to mean that $N = p_1 \cdot p_2 \cdot p_3 \cdots p_d$ and $i \neq j$ implies $p_i \neq p_j$. Clearly

$$q^d \leq N \text{ and } N \leq p^d,$$

so that

$$d \leq \log_q N \text{ and } \log_p N \leq d,$$

establishing the desired inequality. It should be noted that this proof holds also for cases in which the p_i are not necessarily distinct, that is, where N is simply the product of any d primes.

Also solved by **David Anderson,** University of Virginia, Charlottesville, **Frank P. Battles,** Massachusetts Maritime Academy, Buzzards Bay, **Soumya Kanti Das Bhaumik,** Angelo State University, San Angelo, TX, **William Chau,** Primary Knowledge, Inc., New York, NY, **Brian Clester,** Perry, GA, **Jesse Crawford,** Angelo State University, San Angelo, TX, **Mark Evans,** Louisville, KY, **Victor G. Feser,** University of Mary, Bismarck, ND, **Richard I. Hess,** Rancho Palos Verdes, CA, **Peter A. Lindstrom,** Batavia, NY, **David E. Manes,** SUNY College at Oneonta, **Joseph Martin,** Alma College, MI, **Shiva K. Saksena,** University of North Carolina at Wilmington, **H.-J. Seiffert,** Berlin, Germany, **SUNY Fredonia Student Group,** NY, **Leon Vargian,** Midland Park High School, NJ, **J. Ernest Wilkins, Jr.,** Clark Atlanta University, GA, and **Rex H. Wu,** Brooklyn, NY.

Editorial note: I regret the poor wording of the proposal. Several solvers interpreted it differently, allowing each "distinct" prime factor to occur more than once so that N has more than d factors. The theorem is not true with that interpretation. Many solvers proved the result alluded to by the featured solver.

968. [Fall 1999] *Proposed by Doru Popescu Anastasiu, Liceul Radu Greceanu, Slatina, Romania.*

Determine all real numbers x and y such that

$$16x^2 + 21y^2 - 12xy - 4x - 6y + 1 = 0.$$

I. *Solution by* **Soumya Kanti Das Bhaumik,** *Student, Angelo State University, San Angelo, Texas.*

If we complete the square in x and simplify, the given equation becomes

$$(8x - 1 - 3y)^2 + 3(5y - 1)^2 = 0,$$

which requires that $8x - 1 - 3y = 0$ and $5y - 1 = 0$. The solution is $x = 1/5$, $y = 1/5$.

Similar problems may be constructed by starting with a pair of positive numbers p and q and a pair of lines $ax + by - c = 0$ and $dx + ey - f = 0$ that intersect in exactly one point. Then expand and collect terms in the equation $p(ax + by - c)^2 + q(dx + ey - f)^2 = 0$.

II. *Solution by* **Megan Foster,** *student, Alma College, Alma, Michigan.*

Let $f(x, y)$ denote the left side of the given equation. Its first partial derivatives are

$$f_x = 32x - 12y - 4 \text{ and } f_y = 42y - 12x - 6$$

and these are both equal to zero at $x = y = 1/5$. We find that $f(1/5, 1/5) = 0$ and at this point the second derivative test yields

$$f_{xx}f_{yy} - f_{xy}^2 = (32)(42) - (-12)^2 = 1200 > 0,$$

so $(1/5, 1/5)$ is the absolute minimum of f and hence its only zero.

Also solved by **Alma College Problem Solving Group,** MI, **Frank P. Battles,** Massachusetts Maritime Academy, Buzzards Bay, **Kenneth B. Davenport,** Frackville, PA, **George**

P. Evanovich, Saint Peter's College, Jersey City, NJ, **Mark Evans,** Louisville, KY, **Chris Farmer,** Northwest Missouri State University, Maryville, **Robert C. Gebhardt,** Hopatcong, NJ, **Richard I. Hess,** Rancho Palos Verdes, CA, **Joe Howard,** New Mexico Highlands University, Las Vegas, **Murray S. Klamkin,** University of Alberta, Canada, **Mark Kowal,** Alma College, MI, **David E. Manes,** SUNY College at Oneonta, **Yoshinobu Murayoshi,** Okinawa, Japan, **William H. Peirce,** Rangeley, ME, **Cecil Rousseau,** University of Memphis, TN, **Shiva K. Saksena,** University of North Carolina at Wilmington, **H.-J. Seiffert,** Berlin, Germany, **J. Ernest Wilkins, Jr.,** Clark Atlanta University, GA, **Rex H. Wu,** Brooklyn, NY, **Monte J. Zerger,** Adams State College, Alamosa, CO, and the **Proposer.**

969. [Fall 1999] *Proposed by Robert C. Gebhardt, Hopatcong, New Jersey.*
Find $y(x)$ if

$$(e^{-x})\frac{d^2y}{dx^2} + (e^x)y = 0.$$

Solution by **Benjamin Landon,** *student, University of Central Florida, Orlando, Florida.*

Substitute $t = e^x$ to get the differential equation

$$t^2\frac{d^2y}{dt^2} + t\frac{dy}{dt} + t^2y = 0.$$

This is Bessel's differential equation of order 0, whose solution is

$$y(t) = c_1J_0(t) + c_2Y_0(t),$$

where c_1 and c_2 are constants and J_0 and Y_0 are Bessel functions of order 0 of the first and second kinds, respectively. Since $t = e^x$, the solution we seek is

$$y(t) = c_1J_0(e^x) + c_2Y_0(e^x).$$

Also solved by **Alma College Problem Solving Group,** MI, **Frank P. Battles,** Massachusetts Maritime Academy, Buzzards Bay, **Murray S. Klamkin,** University of Alberta, Canada, **Cecil Rousseau,** University of Memphis, TN, **J. Ernest Wilkins, Jr.,** Clark Atlanta University, GA, and the **Proposer.**

970. [Fall 1999, corrected Spring 2000] *Proposed by Ice B. Risteski, Skopje, Macedonia.*

Show that

$$\int_0^{\pi/4}\frac{\cos x\ln\sin x}{\sqrt{\sin x\cos 2x}}dx = -\frac{\pi+\ln 2}{4\sqrt[4]{2}}B\left(\frac{1}{4},\frac{1}{2}\right)$$

and

$$\int_0^{\pi/4}\frac{\cos x\ln\cos 2x}{(\cos 2x)^{3/4}}dx = -\frac{\pi}{2\sqrt{2}}B\left(\frac{1}{4},\frac{1}{2}\right),$$

where $B(m,n) = \Gamma(m)\Gamma(n)/\Gamma(m+n) = \int_0^1 x^{m-1}(1-x)^{n-1}dx$ is the Beta function.

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

Each of the following integrals holds for all complex numbers m and n with positive real parts. It is known ([1], p. 570) that

$$\int_0^1 t^{m-1}(1-t)^{n-1}\ln t\,dt = (\psi(m) - \psi(m+n))B(m,n), \tag{0.1}$$

where $\psi(x) = \Gamma'(x)/\Gamma(x)$ denotes the Digamma function. The substitution $t = 2\sin^2(x)$ gives

$$\int_0^{\pi/4}\sin^{2m-1}(x)\cos^{n-1}(2x)\cos(x)\ln(2\sin^2(x))dx = \frac{\psi(m)-\psi(m+n)}{2^{m+1}}B(m,n),$$

where we have used the trigonometric relation $1 - 2\sin^2(x) = \cos(2x)$.

The same substitution in

$$\int_0^1 t^{m-1}(1-t)^{n-1}dt = B(m,n)$$

yields

$$\int_0^{\pi/4}\sin^{2m-1}(x)\cos^{n-1}(2x)\cos(x)dx = \frac{1}{2^{m+1}}B(m,n).$$

It follows that

$$\int_0^{\pi/4}\sin^{2m-1}(x)\cos^{n-1}(2x)\cos(x)\ln(\sin(x))dx = \frac{\psi(m)-\psi(m+n)-\ln 2}{2^{m+2}}B(m,n).$$

Since ([1], p. 954) $\psi(3/4) - \psi(1/4) = \pi$, this formula with $m = 1/4$ and $n = 1/2$ gives

$$\int_0^{\pi/4}\frac{\cos x\ln\sin x}{\sqrt{\sin x\cos 2x}}dx = -\frac{\pi+\ln 2}{4\sqrt[4]{2}}B\left(\frac{1}{4},\frac{1}{2}\right),$$

the corrected version of the first desired integral evaluation.

With the substitution $t = \cos(2x)$, equation 0.1 becomes

$$\int_0^{\pi/4}\cos^{m-1}(2x)\sin^{2n-1}(x)\cos(x)\ln(\cos(2x))dx = -\frac{\psi(m+n)-\psi(m)}{2^{n+1}}B(m,n),$$

where we have used $1 - \cos(2x) = 2\sin^2(x)$ and $\sin(2x) = 2\sin(x)\cos(x)$. Taking $m = 1/4$ and $n = 1/2$, we obtain the second required integral evaluation.

Reference:

1. I. S. GRADSHTEYN and I. M. RYZHIK, "Table of Integrals, Series, and Products," 5th ed., Academic Press, 1994.

Also solved by **Kenneth B. Davenport,** Frackville, PA, **Cecil Rousseau,** University of Memphis, TN, **J. Ernest Wilkins, Jr.,** Clark Atlanta University, GA, and the **Proposer.**

971. [Fall 1999] *Proposed by Richard I. Hess, Rancho Palos Verdes, California.*
Find an integer-sided obtuse triangle with acute angles in the ratio 7/5.

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

Let ABC be a triangle with acute angles A and B in the ratio 7 to 5. Thus $A = 7\theta$ and $B = 5\theta$, whence $C = 180° - 12\theta$, where we measure all angles in degrees. Because C is obtuse, $0° < \theta < 7.5°$. Since the sides of a triangle are proportional to the sines of their opposite angles, there is a constant k such that the sides a, b, and c are given by

$$a = k\sin 7\theta = k\sin\theta(64\cos^6\theta - 80\cos^4\theta + 24\cos^2\theta - 1),$$

$$b = k\sin 5\theta = k\sin\theta(16\cos^4\theta - 12\cos^2\theta + 1),$$

and

$$\begin{aligned} c &= k\sin(180^\circ - 12\theta) = k\sin 12\theta \\ &= k\sin\theta(2048\cos^{11}\theta - 5120\cos^9\theta + 4608\cos^7\theta - 1792\cos^5\theta + 280\cos^3\theta - 12\cos\theta). \end{aligned}$$

Let r and s be positive integers, let $\cos\theta = r/2s$, and let $k = s^{11}/\sin\theta$ to get

$$a = s^5(r^6 - 5r^4s^2 + 6r^2s^4 - s^6),$$

$$b = s^7(r^4 - 3r^2s^2 + s^4) = s^7(r^2 - rs - s^2)(r^2 + rs - s^2),$$

and

$$\begin{aligned} c &= r(r^{10} - 10r^8s^2 + 36r^6s^4 - 56r^4s^6 + 35r^2s^8 - 6s^{10}) \\ &= r(r^2 - s^2)(r^2 - 2s^2)(r^2 - 3s^2)(r^4 - 4r^2s^2 + s^4). \end{aligned}$$

To find r and s such that angle C is obtuse, that is, with $0^\circ < \theta < 7.5^\circ$, we must have $\cos 7.5^\circ < r/(2s) < 1$. Since $\cos 7.5^\circ \approx 0.991445$, $r/(2s)$ is close to 1, so $1 - r/(2s)$ is close to zero and its reciprocal must be large; greater than $1/(1 - \cos 7.5^\circ) \approx 116.9$. Thus we take $2s = 118$ and $r = 117$, so $s = 59$. The sides for this triangle are 21-digit integers. They and their factorizations are

$$a = 41 \cdot 59^5 \cdot 97 \cdot 4507 \cdot 14,323 = 183{,}542{,}735{,}119{,}347{,}169{,}603,$$

$$b = 5 \cdot 59^7 \cdot 71 \cdot 241 \cdot 661 = 140{,}737{,}857{,}915{,}018{,}789{,}245,$$

and

$$c = 2^7 \cdot 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 29 \cdot 31^2 \cdot 263 \cdot 541 \cdot 16{,}921 = 232{,}117{,}687{,}881{,}273{,}946{,}752.$$

Since $\cos\theta = r/(2s) = 117/118$, then $\theta \approx 7.464553^\circ$ and the angles for this triangle are $A \approx 52.251871^\circ$, $B \approx 37.322765^\circ$, and $C \approx 90.425364^\circ$.

Also solved by **Cecil Rousseau,** University of Memphis, TN, and the **Proposer.** One incorrect answer was received.

Editorial note: Both Rousseau and the Proposer used $\cos\theta = p/q$. The Proposer used $q = 117$, the smallest permissible value, and $p = 116$, obtaining triangle sides of length 24 digits, and Roussseau used $p/q = 199/200$ to obtain sides 23 digits long. Using an even value for q allows for the division by enough powers of 2 to shorten a, b, and c significantly.

972. [Fall 1999] *Proposed by Paul S. Bruckman, Berkeley, California.*

Given three non-collinear points A, B, and C in the complex plane, determine I, the incenter of triangle ABC as a "weighted average" of these points.

Solution by **Rex H. Wu,** *Brooklyn, New York.*

In the accompanying figure let the triangle be ABC and let A, B, and C be the complex affixes of the vertices. Let a, b, and c be the (positive real) lengths of the sides opposite these vertices. Let the internal bisector of angle C cut the opposite side at D and let the internal bisector of angle A cut CD at P. Then P is the desired incenter of triangle ABC. Let the lengths of AD and DB be x and y respectively.

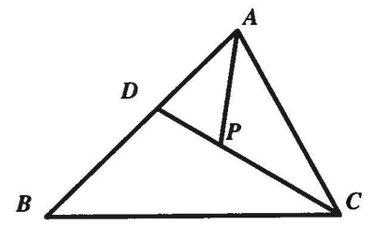


FIG. 0.1. *The incenter.*

Since it is known that the bisector of an angle of a triangle cuts the opposite side into segments proportional to the adjacent sides, then $\frac{b}{a} = \frac{AD}{DB} = \frac{x}{y} = \frac{D-A}{B-D}$ and hence $D = \frac{aA+bB}{a+b}$ and $x = \frac{bc}{a+b}$.

We now apply this same result to triangle ACD with angle bisector AP to find that

$$P = \frac{xC + bD}{x + b} = \frac{\frac{bc}{a+b}C + \frac{b}{a+b}(aA + bB)}{\frac{bc}{a+b} + b} = \frac{aA + bB + cC}{a + b + c}.$$

Also solved by **Murray S. Klamkin,** University of Alberta, Canada, **William H. Peirce,** Rangeley, ME, **Cecil Rousseau,** University of Memphis, TN, **H.-J. Seiffert,** Berlin, Germany, and the **Proposer.**

Editorial comment: Both Klamkin and Seiffert pointed out that this result is well known. It also appears as an exercise in class notes I wrote for a course entitled Complex Numbers for Teachers that I first taught in 1973.

973. [Fall 1999] *Proposed by Ayoub B. Ayoub, Pennsylvania State University, Abington, Pennsylvania.*

Prove that $a_{n+1} = 2a_n + a_{n-1}$, given that $a_0 = 0$ and

$$a_n = \binom{n}{1} + 2\binom{n}{3} + 2^2\binom{n}{5} + 2^3\binom{n}{7} + \cdots.$$

Solution by **William G. Hillegass, Jr.,** *student, Stanton College Preparatory School, Jacksonville Beach, Florida.*

The recurrence equation for $a_{n+1} = 2a_n + a_{n-1}$ is $x^2 - 2x - 1 = 0$, which has zeros $u = 1 + \sqrt{2}$ and $v = 1 - \sqrt{2}$. Thus, if an a_n is any linear combination of u^n and v^n, the recurrence equation is satisfied, a fact that is easily checked by mathematical induction.

For positive integral n the binomial expansion yields

$$(1+x)^n = 1 + x + \binom{n}{2}x^2 + \binom{n}{3}x^3 + \binom{n}{4}x^4 + \cdots,$$

which sum terminates since $\binom{n}{k} = 0$ whenever $k > n$. Now replace x by $-x$ in this sum and subtract the two equations to get

$$(1+x)^n - (1-x)^n = 2(x + \binom{n}{3}x^3 + \binom{n}{5}x^5 + \binom{n}{7}x^7 + \cdots).$$

Finally, replace x by $\sqrt{2}$ and divide both sides by $2\sqrt{2}$ to obtain

$$\frac{(1+\sqrt{2})^n-(1-\sqrt{2})^n}{2\sqrt{2}} = 1+\binom{n}{3}2+\binom{n}{5}2^2+\binom{n}{7}2^3+\cdots.$$

which is the desired sum. Since the left side is a linear combination of u^n and v^n and therefore obeys the desired recursion equation, the proof is complete.

Also solved by **Alma College Problem Solving Group,** MI, **Frank P. Battles,** Massachusetts Maritime Academy, Buzzards Bay, **Kenneth B. Davenport,** Frackville, PA, **Charles R. Diminnie,** Angelo State University, San Angelo, TX, **Mark Evans,** Louisville, KY, **Murray S. Klamkin,** University of Alberta, Canada, **David E. Manes,** SUNY College at Oneonta, **William H. Peirce,** Rangeley, ME, **Cecil Rousseau,** University of Memphis, TN, **Shiva K. Saksena,** University of North Carolina at Wilmington, **H.-J. Seiffert,** Berlin, Germany, **Rex H. Wu,** Brooklyn, NY, and the **Proposer.**

974. [Fall 1999] *Proposed by Kenichiro Kashihara, Sagamihara, Kanagawa, Japan.*

Given any positive integer n, the Pseudo-Smarandache function $Z(n)$ is the smallest integer m such that n divides

$$\sum_{k=1}^{m} k.$$

a) Solve the Diophantine equation $Z(x) = 8$.

b) Show that for any positive integer p the equation $Z(x) = p$ has solutions.

*c) Show that the equation $Z(x) = Z(x+1)$ has no solutions.

*d) Show that for any given positive integer r there exists an integer s such that the absolute value of $Z(s) - Z(s+1)$ is greater than r.

Editorial note: **C. Bryan Dawson,** Union University, Jackson, Tennessee, has pointed out that this same problem was proposed by the same proposer in the Spring 1997 issue of The Pentagon as Problem 509. Its solution appears in the Spring 1998 issue, pp. 56-58. **H.-J. Seiffert,** Berlin, Germany, found parts (b), (c), and (d) as Problem 4625 by the same proposer in School Science and Mathematics 98.5, pp. 275-276, 1998.

Also solved by **David Anderson,** University of Virginia, Charlottesville, **William Chau** (parts (a) and (b)), Primary Knowledge, Inc., New York, NY, **Stephen I. Gendler,** Clarion University of Pennsylvania, **Mark Evans,** (parts (a) and (b)), Louisville, KY, **Richard I. Hess,** Rancho Palos Verdes, CA, **William G. Hillegass, Jr.,** (parts (c) and (d)), Stanton College Preparatory School, Jacksonville Beach, FL, **David E. Manes,** SUNY College at Oneonta, **H.-J. Seiffert,** (part (a)), **Rex H. Wu,** Brooklyn, NY, and the **Proposer** (parts (a) and (b)).

975. [Fall 1999] *Proposed by Doru Popescu Anastasiu, Liceul Radu Greceanu, Slatina, Romania.*

For any given fixed positive integer n, determine the positive integers $x_1, x_2, \ldots, x_n$ such that

$$x_1+2(x_1+x_2)+3(x_1+x_2+x_3)+\cdots+n(x_1+x_2+\cdots+x_n) = \frac{2n^3+3n^2+7n}{6}.$$

I. *Solution by* **Karthik Gopalrtanam,** *student, Angelo State University, San Angelo, Texas.*

If $n = 1$, the obvious solution is $x_1 = 2$.

For $n \geq 2$, the right side of the equation becomes

$$\frac{2n^3+3n^2+n}{6}+n = \frac{n(n+1)(2n+1)}{6}+n = (1^2+2^2+\cdots+n^2)+n.$$

Subtracting this new expression from each side of the given equation produces

$$(x_1-1)+[2(x_1+x_2)-2^2]+[3(x_1+x_2+x_3)-3^2]+\cdots+[n(x_1+x_2+\cdots+x_n)-(n^2+n)] = 0$$

or

$$(x_1-1)+2(x_1+x_2-2)+3(x_1+x_2+x_3-3)+\cdots+n(x_1+x_2+\cdots+x_n-n-1) = 0.$$

If the x_k are all equal to 1, the least positive integer, then each group of terms on the left is 0 except for the last group, which equals $-n$. If x_n is increased to 2, then the last group becomes 0 and the equation is satisfied. So $x_1 = x_2 = x_3 = \cdots = x_{n-1} = 1$ and $x_n = 2$ is a solution. If any $x_k > 1$ for $k < n$, or if $x_n > 2$, then the left side is positive. Hence there is no other solution.

II. *Solution by* **Joe Howard,** *New Mexico Highlands University, Las Vegas, New Mexico.*

We determine positive numbers x_k, not necessarily integers, such that the given equation is true for every positive integer n.

By direct calculation, $x_1 = 2$, $x_2 = 1/2$, $x_3 = 5/6$, $x_4 = 11/12$, ..., $x_n = [n(n-1)-1]/[n(n-1)]$ for $n > 1$. Then $x_1+x_2+\cdots+x_n = (n^2+1)/n$. The induction step to prove this last statement is

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

The given equation then becomes

$$2+5+10+\cdots+n\left(\frac{n^2+1}{n}\right) = \frac{2n^3+3n^2+7n}{6}.$$

The following induction step proves this statement and establishes our result:

$$\frac{2n^3+3n^2+7n}{6}+[(n+1)^2+1] = \frac{2n^3+3n^2+7n}{6}+\frac{6n^2+12n+12}{6}$$

$$= \frac{2n^3+9n^2+19n+12}{6} = \frac{2(n+1)^3+3(n+1)^2+7(n+1)}{6}.$$

Also solved by **Alma College Problem Solving Group,** MI, **David Anderson,** University of Virginia, Charlottesville, **Frank P. Battles,** Massachusetts Maritime Academy, Buzzards Bay, **William Chau,** Primary Knowledge, Inc., New York, NY, **Charles R. Diminnie,** Angelo State University, San Angelo, TX, **George P. Evanovich,** Saint Peter's College, Jersey City, NJ, **Mark Evans,** Louisville, KY, **Yu Gan,** Loch Raven High School, Baltimore, MD, **Robert C. Gebhardt,** Hopatcong, NJ, **Steve Haas,** Harvey Mudd College, Claremont, CA, **Richard I. Hess,** Rancho Palos Verdes, CA, **Murray S. Klamkin,** University of Alberta, Canada, **Peter A. Lindstrom,** Batavia, NY, **David E. Manes,** SUNY College at Oneonta, **Yoshinobu Murayoshi,** Okinawa, Japan, **William H. Peirce,** Rangeley, ME, **Cecil Rousseau,** University of Memphis, TN, **Shiva K. Saksena,** University of North Carolina at Wilmington, **H.-J. Seiffert,** Berlin, Germany, **J. Ernest Wilkins, Jr.,** Clark Atlanta University, GA, **Rex H. Wu,** Brooklyn, NY, **Monte J. Zerger,** Adams State College, Alamosa, CO, and the **Proposer.**

976. [Fall 1999] *Proposed by Rajindar S. Luthar, University of Wisconsin Center, Janesville, Wisconsin.*

If $x + y + z + t = \pi$, prove that

$$\tan(x + y)\tan(z + t) > 27 \cot x \cot y \cot z \cot t.$$

Editorial note: **George P. Evanovich,** Saint Peter's College, Jersey City, NJ, **Steven Haas,** Harvey Mudd College, Claremont, CA, **Richard I. Hess,** Rancho Palos Verdes, CA, **William Hillegass,** Stanton College Preparatory School, Jacksonville Beach, FL, **Murray S. Klamkin,** University of Alberta, Canada, **J. Ernest Wilkins, Jr.,** Clark Atlanta University, GA, and **Rex H. Wu,** Brooklyn, NY, all found values which violate the stated inequality. Hence, the proposed inequality is not a theorem and this problem is withdrawn . As partial compensation to our readers, perhaps, note that each of the Fall 1999 and the Spring 2000 issues contained 14 proposals, one more than the usual number.

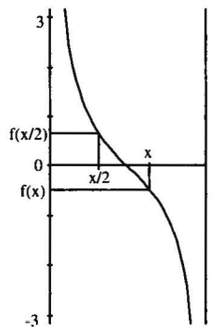
977. [Fall 1999] *Proposed by Rajindar S. Luthar, University of Wisconsin Center, Janesville, Wisconsin.*

If A, B, and C are the angles of a triangle, then prove that

$$\cot\frac{A}{2} + \cot\frac{B}{2} + \cot\frac{C}{2} > \cot A + \cot B + \cot C.$$

Solution by **Alma College Problem Solving Group,** *Alma College, Alma, Michigan.*

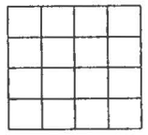
Proof without words:



Also solved by **Alma College Problem Solving Group** (second solution), **Miguel Amengual Covas,** Cala Figuera, Mallorca, Spain, **John Boyer,** Alma College, MI, **Justin H. Brehm,** Alma College, MI, **Kenneth B. Davenport,** Frackville, PA, **Charles R. Diminnie,** Angelo State University, San Angelo, TX, **George P. Evanovich,** Saint Peter's College, Jersey City, NJ, **Mark Evans,** Louisville, KY, **Ryan Fowler,** Alma College, MI, **Yu Gan,** Loch Raven High School, Baltimore, MD, **Phil Harger,** Alma College, MI, **Richard I. Hess,** Rancho Palos Verdes, CA, **William Hillegass,** Stanton College Preparatory School, Jacksonville Beach, FL, **Joe Howard,** New Mexico Highlands University, Las Vegas, **Murray S. Klamkin,** University of Alberta, Canada, **Peter A. Lindstrom,** Batavia, NY, **Karli Lopez,** Alma College, MI, **David E. Manes,** SUNY College at Oneonta, **Justin Modrzynski,** Alma College, MI, **Yoshinobu Murayoshi,** Okinawa, Japan, **Jennifer Oglenski,** Alma College, MI, **Cecil Rousseau,** University of Memphis, TN, **Shiva K. Saksena,** University of North Carolina at Wilmington, **H.-J. Seiffert,** Berlin, Germany, **Paul Vitantonio,** Alma College, MI, **Justin Wilcoxen,** Alma College, MI, **J. Ernest Wilkins, Jr.,** Clark Atlanta University, GA, **Rex H. Wu,** Brooklyn, NY, and the **Proposer.**

978. [Fall 1999] *Proposed by Richard I. Hess, Rancho Palos Verdes, California.*

In the array below place sixteen digits to form eight not necessarily distinct squares without using the digit zero. The answer is unique.



Solution by **David E. Manes,** *SUNY College at Oneonta, Oneonta, New York.*

The unique solution is

2	1	1	6
1	2	2	5
1	2	9	6
6	5	6	1

All square numbers terminate in 0, 1, 4, 5, 6, or 9. Of the 44 four-digit squares not containing a zero, only 1156, 1444, and 6561 can be used for the last column or for the last row since they are composed of only the permissible terminal digits 1, 4, 5, 6, and 9. Since these three numbers have different terminal digits, then the last row and the last column are equal. We try each possibility. For the last row and last column using 1156, the only possible choices for the first row or column are 1521, 1681, 3481, 3721, 4761, 6241, 6561, 7921, and 8281. These numbers start with 1, 3, 4, 6, 7, or 8. Each second digit is 2, 4, 5, 6, 7, or 9. Place one of these numbers in the first row. The number in the second column must start with the second digit of the number in the first row. Then only 1681, 3481, 3721, 4761 could be used in the first row. Since all squares that end in 5 must end in 25, the number in the 3rd row and 3rd column is 2. The third column is 2x25, 6x25, or 8x25, none of which is a square for a nonzero digit x. Similarly, 1444 is eliminated. Only 6561 remains to be considered, and all possibilities but the solution listed above are readily eliminated.

Also solved by **Alma College Problem Solving Group,** MI, **Charles D. Ashbacher,** Charles Ashbacher Technologies, Hiawatha, IA, **Patrick Costello,** Eastern Kentucky University, Richmond, **Kenneth B. Davenport,** Frackville, PA, **Charles R. Diminnie,** Angelo State University, San Angelo, TX, **Mark Evans,** Louisville, KY, **Victor G. Feser,** University of Mary, Bismarck, ND, **Rex H. Wu,** Brooklyn, NY, **Yeepay Yang,** Massachusetts Academy of Math and Science, Worcester, and the **Proposer.**

Editorial comment: By allowing zeros, **Rex H. Wu** found fourteen additional solutions, only one of which is not symmetric about its main diagonal. The rows of that solution are 8281, 1444, 0064, and 0144. Its columns are, of course, 8100, 2401, 8464, and 1444.

***979.** [Fall 1999] *Proposed by Murray S. Klamkin, University of Alberta, Edmonton, Alberta, Canada.*

Dedicated to Professor M. V. Subbarao on the occasion of his 78th birthday. Do there exist an infinite number of triples of consecutive positive integers such that one of them is prime, another is a product of two primes, and the third is a product of three primes? Two such examples are 6, 7, 8 and 77, 78, 79.

Comments by **J. Ernest Wilkins, Jr.,** *Clark Atlanta University, Atlanta, Georgia.*

Although we do not settle the proposed question rigorously, there is a long outstanding conjecture of Bateman and Horn [1] that implies an affirmative answer. Moreover, a negative answer to the proposed question would disprove the Bateman-Horn conjecture.

Let V_1 be the set of all positive integers v such that $4v+1$, $18v+5$, and $36v+11$ are all primes. Then the triple of consecutive integers x_1, x_1+1, x_1+2, in which $x_1 = 9(4v+1)$, is clearly a triple of the desired kind. With Bateman and Horn we define the quantity C_1 so that

$$C_1 = \prod_p (1-p^{-1})^{-3}[1-p^{-1}w(p)],$$

in which $w(p)$ is the number of distinct solutions (mod p) to the congruence

$$(4v+1)(18v+5)(36v+11) \equiv 0 (\text{mod } p),$$

and the product extends over all primes p. It is clear that $w(2) = 0$, $w(3) = 1$, and $w(p) = 3$ if $p > 3$. The infinite product converges to a positive limit because no factor vanishes, $(1-p^{-1})^{-3}(1-3p^{-1}) = 1+0(p^{-2})$, and the infinite series $\sum_p p^{-2}$ converges. The Bateman-Horn conjecture in these circumstances is that the number of elements of V that do not exceed a specified integer n is asymptotic for large n to

$$C_1 \int_2^n (\log y)^{-3} dy. \tag{0.2}$$

If the conjecture is true, it follows from the divergence of the integral (0.2) and the positivity of C_1 that V_1 has infinitely many elements. Hence, there are infinitely many triples of the kind described in the proposed question.

Let us define P_{abc} to be the set of triples of consecutive integers x, $x+1$, $x+2$ for which x, $x+1$, $x+2$ are the products of a, b, and c primes, respectively. We have just shown that the set P_{321} is infinite when the Bateman-Horn conjecture is true. Now let V_2 be the set of positive integers v such that $4v+3$, $18v+13$, and $36v+35$ are all primes, V_3 the set where $9v+5$, $12v+7$, and $36v+19$ are all primes, and V_4 the set where $9v+1$, $12v+1$, and $36v+5$ are all primes. Let $x_2 = 36v+25$, $x_3 = 36v+19$, and $x_4 = 36v+3$. Then x_2, x_2+1, x_2+2 is a triple P_{123} when v is in V_2, x_3, x_3+1, x_3+2 is a triple P_{132} when v is in V_3, and x_4, x_4+1, x_4+2 is a triple P_{231} when v is in V_4. A repetition of the analysis of the preceding paragraph shows that each of the sets V_2, V_3, and V_4 is infinite when the Bateman-Horn conjecture is valid. Hence sets P_{123}, P_{132}, and P_{231} are also infinite.

Nevertheless, the sets P_{213} and P_{312} are finite. In fact, the triple x, $x+1$, $x+2$ is in P_{312} if and only if $x = 4u$, where u is a prime such that $2u+1$ and $4u+1$ are also primes. If $u \equiv 1$ (mod 3), then $2u+1 \equiv 0$ (mod 3), and if $u \equiv 2$(mod 3), then $4u+1 \equiv 0$ (mod 3). Hence, only when $u = 3$ are u, $2u+1$, and $4u+1$ all primes. We conclude that P_{312} consists of the unique triple 12, 13, 14. Similarly, x, $x+1$, $x+2$ is in P_{213} if and only if $x = 2(2u-1)$, where u, $2u-1$, and $4u-1$ are all primes. If $u \equiv 0$ (mod 3), then u cannot be a prime unless $u = 3$. If $u \equiv 1$ (mod 3), then $4u-1 \equiv 0$ (mod 3) and $4u-1$ is not prime because $u \neq 1$. If $u \equiv 2$ (mod 3), then $2u-1 \equiv 0$ (mod 3). Hence $2u-1$ cannot be a prime unless $u = 2$. We conclude that the only triples in P_{213} are 6, 7, 8 and 10, 11, 12.

Of course we do not need the full force of the Bateman-Horn conjecture. That conjecture deals with an arbitrary number of polynomials of arbitrary degree, whereas

we need only consider three linear polynomials. Moreover, the conjecture states the asymptotic formula (0.2), and we need only know that one of the sets V_1, V_2, V_3, and V_4 has an infinite number of elements. To the best of our knowledge, it is not known if even the much weaker conjecture needed for our purposes is true or is false.

Reference: 1. PAUL T. BATEMAN and ROGER A. HORN, *A heuristic asymptotic formula concerning the distribution of prime numbers,* Mathematics of Computation, vol. 16, 79 (1962) 363-367.

Editorial note: **Richard I. Hess,** Rancho Palos Verdes, CA, offered an argument showing it is highly probable that the conjecture is true, that "testing enough large numbers should always produce arbitrarily large triples of consecutive numbers" that satisfy the conjecture.

MATHACROSTIC

The MATHACROSTIC in this issue has been contributed by Dan Hurwitz.

a. A basic form of valid reasoning (2 wds.)

b. Frequency given by the number of occurrences in a sample

c. Eg. "All Men are mortal ..."

d. Ways to represent statements by metaexpressions

e. Onto function (2 wds.)

f. Originally defined in bronze

g. First coordinate

h. The ___ ___ points such that ...

i. Something true of everything (2 wds.)

j. Injective homomorphism

k. Type of number sorting

l. Medium change does this to light

m. Many have a finite number of states

n. Estimating an intermediate value

o. What one does to like terms

p. Probabilist's experimental technique

q. Categories with the same objects, reversed morphisms

r. Homological diagram extension

s. Not in Inn(G) (2 wds.)

t. Great figure in measure theory

u. Fruity union of cycle free graphs

v. Script sometimes used in logic

w. Component in one non-binary universe

145 024 090 128 051 038 078 062 117

006 158

177 047 069 139 021 098 081 155

056 002 031 101 122 022 082 146 070

073 179 009 087 041 103 153 120

166 129 149 111 138 075 026

187 036 140 059

020 115 161 060 178 141 085 046

116 137 035 003 152 127 170

007 184 061 107 015 172 072 113 028 141

043 099 121 168

093 118 156 055 011 133 143 076 033

121 049 001 086 037 106

126 084 011 039 164 160 063

131 068 008 048 083 109 095 157

151 058 027 017 088 182 114 042 071

165 005 132 105

054 030 079 175 159 065 100

050 183 150 130

185 097 029 135 119 061 018 173

112 012 045 148 032 091 180

040 025 162 080 023 171 123 147 067

016 096 176 052 154 110 001 136

104 010 041 174 077 125 066 089

181 163 071 142 057 108 094

186 169 019 134 031 092

102 053 013 167

■	001k	002c	■	003h	004s	005n	006a	007i	■	008m	009d	010t	■	011l
012r	013w	014j	015i	016s	017n	018q	019v	020g	021b	■	022c	023s	024a	025s
026e	■	027n	028i	029q	030o	031c	032r	033j	034v	035h	036f	037k	■	038a
039l	040s	041t	042n	043i	044d	045r	■	046g	047b	048m	049k	050p	■	051a
052s	053w	054o	055j	056c	■	057u	058n	059f	■	060g	061i	062a	063l	064q
065o	066t	067s	068m	069b	■	070c	071n	072i	073d	■	074u	075e	076j	■
077t	078a	079o	080s	081b	082c	083m	084l	085g	■	086k	087d	■	088n	089t
090a	091r	092v	093j	094u	■	095m	096s	■	097q	098b	099i	100o	101c	102w
■	103d	104t	105n	106k	107i	108u	109m	110s	111e	■	112r	113i	114n	115g
116h	117a	118j	119q	■	120d	121k	122c	123s	124i	■	125t	126l	127h	128a
129e	130p	■	131m	132n	133j	■	134v	135q	136s	137h	138e	139b	140f	141i
142u	143j	144g	145a	146c	■	147s	148r	149e	150p	■	151n	152h	■	153d
154s	155b	■	156j	157m	158a	159o	160l	■	161g	162s	163u	164l	165n	166e
167w	168i	■	169v	170h	■	171s	172i	173q	174t	175o	176s	177b	178g	179d
■	180r	181u	182n	183p	184i	185q	186v	187f	■	■	■	■	■	■

Last month's mathacrostic was taken from "The Historical Roots of Elementary Mathematics" by Lucas Bunt, Philip Jones, and Jack Bedient. The full text of the quote is (with the puzzle solution in parentheses):

> "We do know that (the Pythagorean Archytas divided mathematics into four parts: music, arithmetic, astronomy, and geometry. These subjects, called the quadrivium, were later adopted by Plato and Aristotle and became the school curriculum for centuries) - in fact, up until the Renaissance".

Contents