ARTICLES BY TITLE

INDEX TO VOLUME 48 — JANUARY THROUGH DECEMBER, 1975

ARTICLES BY AUTHOR

BOOK REVIEWS

EDITED BY ADA PELUSO, Hunter College of CUNY, and WILLIAM WOOTON, Lake San Marcos, California

Names of authors are in ordinary type; those of reviewers in capitals and small capitals.

PROBLEMS AND SOLUTIONS

EDITED BY DAN EUSTICE, The Ohio State University

PROPOSALS

SOLUTIONS

Quickies and Answers

The page on which Quickies appear is in parentheses following the number of these problems; the page on which the Answers appear is in boldface: 608, 609, 610, 611, 612, 613 (52) (**58**); 614, 615, 616, 617, 618, 619 (116–117) (**122**); 620, 621, 622, 623, 624 (181–182) (**186**); 625, 626, 627 (240) (**248**); 628, 629, 630 (295) (**302–303**).

U.S. POSTAL SERVICE
STATEMENT OF OWNERSHIP, MANAGEMENT AND CIRCULATION
(Act of August 12, 1970: Section 3685, Title 39, United States Code

1. TITLE OF PUBLICATION: MATHEMATICS MAGAZINE
2. DATE OF FILING: SEPT. 9, 1975
3. FREQUENCY OF ISSUE: 5 issues per year
3A. ANNUAL SUBSCRIPTION PRICE: $10.00
4. LOCATION OF KNOWN OFFICE OF PUBLICATION *(Street, city, county, state and ZIP code) (Not printers)*: 1225 Connecticut Ave., NW, Washington, DC 20036
5. LOCATION OF THE HEADQUARTERS OR GENERAL BUSINESS OFFICES OF THE PUBLISHERS *(Not printers)*: 1225 Connecticut Ave., NW, Washington, DC 20036
6. NAMES AND ADDRESSES OF PUBLISHER, EDITOR, AND MANAGING EDITOR

PUBLISHER *(Name and address)*: The Mathematical Association of America, 1225 Connecticut Ave. NW, Washington, DC 20036

EDITOR *(Name and address)*: Prof. Gerhard Wollan, Dept. of Math., Purdue Univ., Lafayette, IN 47906

MANAGING EDITOR *(Name and address)*: Dr. Raoul Hailpern, Math. Ass'n. of America, SUNY at Buffalo, Buffalo, NY 14214

7. OWNER *(If owned by a corporation, its name and address must be stated and also immediately thereunder the names and addresses of stockholders owning or holding 1 percent or more of total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address, as well as that of each individual must be given.)*

NAME	ADDRESS
The Mathematical Association of America, Inc.	1225 Connecticut Avenue NW Washington, DC 20036

8. KNOWN BONDHOLDERS, MORTGAGEES, AND OTHER SECURITY HOLDERS OWNING OR HOLDING 1 PERCENT OR MORE OF TOTAL AMOUNT OF BONDS, MORTGAGES OR OTHER SECURITIES *(If there are none, so state)*

NAME	ADDRESS
none	

9. FOR OPTIONAL COMPLETION BY PUBLISHERS MAILING AT THE REGULAR RATES *(Section 132.121, Postal Service Manual)*

39 U. S. C. 3626 provides in pertinent part: "No person who would have been entitled to mail matter under former section 4359 of this title shall mail such matter at the rates provided under this subsection unless he files annually with the Postal Service a written request for permission to mail matter at such rates."

In accordance with the provisions of this statute, I hereby request permission to mail the publication named in item 1 at the reduced postage rates presently authorized by 39 U. S. C. 3626.

(Signature and title of editor, publisher, business manager, or owner)

10. FOR COMPLETION BY NONPROFIT ORGANIZATIONS AUTHORIZED TO MAIL AT SPECIAL RATES *(Section 132.122 Postal Service Manual) (Check one)*

The purpose, function, and nonprofit status of this organization and the exempt status for Federal income tax purposes [X] Have not changed during preceding 12 months [ ] Have changed during preceding 12 months *(If changed, publisher must submit explanation of change with this statement.)*

11. EXTENT AND NATURE OF CIRCULATION	AVERAGE NO. COPIES EACH ISSUE DURING PRECEDING 12 MONTHS	ACTUAL NUMBER OF COPIES OF SINGLE ISSUE PUBLISHED NEAREST TO FILING DATE
A. TOTAL NO. COPIES PRINTED *(Net Press Run)*	7,120	7,000
B. PAID CIRCULATION 1. SALES THROUGH DEALERS AND CARRIERS, STREET VENDORS AND COUNTER SALES	none	none
2. MAIL SUBSCRIPTIONS		
C. TOTAL PAID CIRCULATION	5,823	5,244
D. FREE DISTRIBUTION BY MAIL, CARRIER OR OTHER MEANS SAMPLES, COMPLIMENTARY, AND OTHER FREE COPIES	30	30
E. TOTAL DISTRIBUTION *(Sum of C and D)*	5,853	5,274
F. COPIES NOT DISTRIBUTED 1. OFFICE USE, LEFT-OVER, UNACCOUNTED, SPOILED AFTER PRINTING	1,267	1,726
2. RETURNS FROM NEWS AGENTS		
G. TOTAL *(Sum of E & F—should equal net press run shown in A)*	7,120	7,000

I certify that the statements made by me above are correct and complete.

SIGNATURE OF EDITOR, PUBLISHER, BUSINESS MANAGER, OR OWNER: Alfred B. Willcox

PS Form Jan 1975 3526 (Page 1) *(See instructions on reverse)*

MATHEMATICS MAGAZINE

CONTENTS

CODEN: MAMGA8

VOLUME 48 • NOVEMBER 1975 • NUMBER 5

THE MATHEMATICAL ASSOCIATION OF AMERICA
1225 Connecticut Avenue, N.W.
Washington, DC 20036

MATHEMATICS MAGAZINE

EDITORIAL CORRESPONDENCE should be sent to the EDITORS-ELECT, J. ARTHUR SEEBACH, JR., and LYNN A. STEEN, Department of Mathematics, St. Olaf College, Northfield, Minnesota 55057. Articles should be typewritten and triple-spaced on $8\frac{1}{2}$ by 11 paper. The greatest possible care should be taken in preparing the manuscript. Authors should submit two copies and keep one copy for protection against possible loss of the manuscript. Figures should be drawn on separate sheets in India ink. They should be appropriately lettered and of a suitable size for photographing.

REPRINT PERMISSION should be requested from LEONARD GILLMAN, Mathematical Association of America, University of Texas, Austin, Texas 78712. (See also the copyright notice below.)

NOTICE OF CHANGE OF ADDRESS and other subscription correspondence should be sent to the Executive Director, A. B. WILLCOX, Mathematical Association of America, Suite 310, 1225 Connecticut Avenue, N. W., Washington, D.C. 20036.

ADVERTISING CORRESPONDENCE should be addressed to RAOUL HAILPERN, Mathematical Association of America, SUNY at Buffalo (University of Buffalo), Buffalo, New York 14214.

THE MATHEMATICS MAGAZINE is published by the Mathematical Association of America at Washington, D.C., bi-monthly except July-August. Ordinary subscriptions are $10 per year. Members of the Mathematical Association of America and of Mu Alpha Theta may subscribe at the special rate of $7.00. Back issues may be purchased, when in print, for $2.00.

Second class postage paid at Washington, D.C. and additional mailing offices.

IMPOSSIBILITY

IAN RICHARDS, University of Minnesota

"While one man was proving it couldn't be done,
another man tried and he did it."
(Children's verse)

How does one prove that something is impossible? Is anything impossible? Yes, of course, some things are. But let us momentarily play the devil's advocate. Conventional folk-wisdom teaches the opposite: that anything can be done if one is clever and tries hard enough. And common experience backs up that point of view. Things once believed to be impossible happen every day. There are two ways that this can come about, and the distinction is important to us here, since we are concerned with theory, not practice. Briefly:

(I) sometimes the thing said to be impossible really isn't;

(II) and sometimes it is. However, even in this latter case it often happens that, *by bending the rules a little bit*, the situation can be altered, and the desired effect thereby achieved.

Type II represents what we call "mathematical impossibility"; type I is mere error. Consider some examples. When my father was a young biologist, working with a (then) new device called the electron microscope, several experts said that it was impossible to cut animal tissue into pieces thin enough for use with this instrument. The idea was that no knife edge, of any known material, was sharp enough to produce the necessary thin sections. My father succeeded in finding a suitable knife. He began by taking a raw carrot, quartered the carrot lengthwise, embedded the material to be cut into the edge of the carrot, and then gently drew a razor blade back and forth along this edge. (Today the same job is done with an instrument called a microtome, which incidentally costs several thousand dollars.)

My father's good fortune in doing what some people said couldn't be done, gives a typical example of type I; the "experts" were simply wrong. More important for our purposes is the type II situation, in which a problem really *is* unsolvable as stated, but a fortuitous change in the initial assumptions allows a "solution" to be found. Perhaps the most famous instance of this in all history is the story of Alexander the Great cutting the Gordian knot. Clearly he changed the rules! At a more mundane level, mathematicians have proved that one cannot trisect an arbitrary angle with ruler and compass; but of course that doesn't prevent engineers from trisecting angles when they need to. Another impossibility theorem (which we will discuss below) involves the "fifteen puzzle". A friend of mine showed this puzzle to his father, and explained that such and such a position could never be attained. His father reached the forbidden position by taking the toy down to his workshop, prying out one of the pieces, and putting it back in a different place — shades of Alexander!

However, some things really are impossible. In the Middle Ages, certain skeptics asked, "If God is omnipotent, can He make an object so heavy that He cannot move it?" The answer given by Thomas Aquinas and others was that "Even omnipotence cannot achieve contradiction."

Of course, this is how mathematicians prove that certain things are impossible. They show that the opposite assumption would lead to a contradiction. We should emphasize, however, that mathematics deals with precisely formulated problems. So, if something is proved impossible, it follows that there will never be a "type I" exception to the law — but, by bending the rules, the whole situation may be altered.

Thus it becomes clear that "impossibility theorems" have little or no practical significance. Nevertheless they are, in the author's opinion, among the most remarkable theorems in mathematics. For they have a certain mystifying quality. If trisecting a general angle *were* possible (as, e.g., bisecting one is), we could easily imagine what such a hypothetical solution would look like: presumably it would look rather like the construction for bisecting an angle, except that it would be more complicated. The reason why an impossibility proof seems mysterious (at least to me), is because of the following question: How do I know that there is not some intricate construction, involving perhaps thousands of steps, which my "proof" has overlooked? Clearly some general principle must be involved. In fact one is, and bringing out this underlying principle in several disparate situations is the main theme of this article.

[*Note.* The practical "uselessness" of impossibility proofs applies only if one takes a rather narrow viewpoint. For some of the *ideas* which have grown out of such investigations — e.g., group theory – have found practical application in other areas.]

A summary of the contents. In this paper we will consider seven problems in which "impossibility" plays a role. These are:

(1) The rook's tour of a chessboard.

(2) The 15-puzzle.

(3) The knight's tour of a tic-tac-toe board.

(4) The magic five-pointed star.

(5) The trisection of an angle.

(6) The irrationality of all "nontrivial" linear combinations of nth roots (e.g., $\sqrt[3]{2}+\sqrt[4]{3}+\sqrt[5]{4}$).

(7) The general quintic equation.

The last three examples above involve Galois theory, and it would require too much space to include their proofs. We will content ourselves with some remarks about them. Also, in this connection, it seems impossible (no pun intended) to improve on the classic books of Artin [**1**] and van der Waerden [**10**].

(Each of these books treats Galois theory from a different viewpoint, and almost all later texts follow one or the other.)

The first four theorems concern elementary puzzles, and here I will give the proofs. However, in case the reader wants to work these problems out for himself, the proofs appear in a separate section, between Example 4 and Example 5. The point of the article is the common thread which runs through all seven examples, from the most elementary to the most advanced.

[*Note.* Although none of the results discussed here are new, one of the proofs is: for the magic star, number (4). In the discussion of this problem, reference is made to an earlier proof (cf. [7].]

Invariants. The common thread running through the seven problems mentioned above is the idea of an invariant. This idea, together with its cousin, the idea of a transformation, lies at the core of much modern mathematics. What is an invariant? To give a precise definition would be outside of the author's competence — the word belongs to logic and philosophy. However, the underlying idea is something like this:

An investigator is faced with a situation which is too complicated to analyze completely. So he finds a particular entity, the "invariant", which incorporates certain particular aspects of the situation. Hopefully the invariant will be easy to calculate. The investigator then shows that, under the sorts of transformations which are allowed in the system, the invariant cannot vary. (This, of course, explains the name.) If "solving" a certain problem would require changing the invariant, then the solution is impossible.

Examples of invariants abound outside of mathematics. Energy, momentum, and angular momentum are standard physical invariants. Stretching a point, the human fingerprint could be called an anatomical invariant. In mathematics, some of the most common invariants are parity (odd versus even) and size (including number, length, area, etc.).

Here it might be worth pointing out that some of these mathematical invariants yield "impossibility theorems" which are so obvious as to escape notice. For example, it is impossible to break a square up into a finite number of triangular pieces, and then reassemble these pieces to form two squares, each having the same area as the original square. (To see the point, try proving this theorem using any idea *except* area.) In the examples which follow, the invariant is sometimes less obvious, but the basic principle is the same.

Examples of impossibility theorems. *Example* 1 (the rook's tour). Imagine a hypothetical piece which is allowed to make only those moves common to both the king and the rook in chess: that is, it can move *one square at a time horizontally or vertically* (but not diagonally, and never more than one square). This piece starts in the upper left-hand corner of a chessboard (see Figure 1) and is required to move over the whole board, occupying each square exactly once (and thus not re-entering the square from which it started). Furthermore, it must end its journey on the square marked "X" in the lower right-hand corner of the board. Prove that this is impossible.

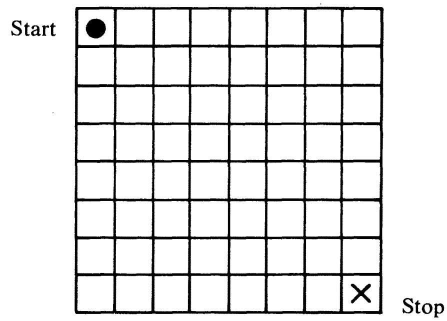


FIG. 1. The rook's tour. The piece indicated by the black dot is restricted to move one square at a time, vertically or horizontally (and not diagonally). It must occupy each square exactly once.

[The solutions to the problems posed by Examples 1 to 4 are given after Example 4.]

Example 2 (the 15-puzzle). A well-known toy involves 15 square pieces placed in a box which is 4 by 4 units on a side. Thus the box has 16 spaces, all but one of which are occupied by the pieces, and one space which is empty (see Figure 2). The pieces are numbered 1 through 15. *They may be moved by sliding an adjacent piece horizontally or vertically into the empty space.* It is forbidden to take any of the pieces out of the box. Show that it is impossible to get from the position shown in Figure 2b to the one in Figure 2a, while staying within the rules of the game.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	empty

FIG. 2a. The desired end position for the 15-puzzle.

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	empty

FIG. 2b. The "other" position. Here the pieces 14 and 15 have been reversed.

Before

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

→

After

1	2	3	4
5	6	7	8
9	10	11	
13	14	15	12

FIG. 2c. A typical move: the number 12 piece slides into the empty square.

Remark. In the old 15-puzzle, popular in the nineteenth century, the pieces were wooden squares, which were loose and could be taken out of the box. These were shaken up and then placed in the box in a random order; the objective was to get the pieces into the "natural" order shown in Figure 2a. However, half of the time this was impossible — if the pieces were placed in the box so that Figure 2b could be reached, then Figure 2a could not. Furthermore (since this puzzle is fairly easy except when it is impossible), Figure 2b would usually be arrived at within a few minutes. Then the frustrated puzzle-solver might spend several fruitless hours trying to "make the last step", i.e., to interchange the 14-piece with the 15-piece. [In modern versions of the puzzle, the "impossible" case is avoided by having the pieces locked in the box with plastic flanges. Unfortunately, then there is a mechanical difficulty: the flanges rub against each other, and the pieces tend to twist and don't slide very well.]

Example 3 (knight's tour of a tic-tac-toe board). Imagine four knights situated on the four corners of a 3×3 playing board. The knights in the lower left and lower right hand corners are colored white and black respectively, while the knights in the two upper corners are both red (see Figure 3). All four pieces move like a knight in chess, except that their moves are confined to the 3×3 board, and *they are not allowed to capture one another.* (Of course, two pieces cannot occupy the same square at the same time.) Prove that it is impossible to interchange the positions of the white and black knights, i.e., to have the white knight in the lower right corner and the black knight in the lower left at the same time. (It is NOT required that the red knights return to their original squares; interchanging the white and black knights is impossible no matter what positions the red knights occupy at the end of the game!)

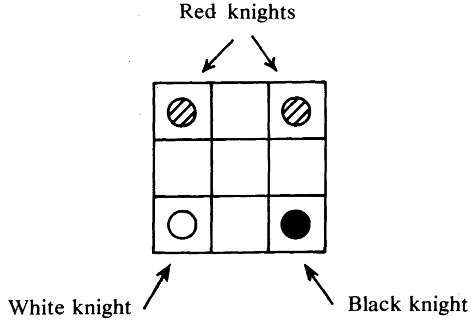


FIG. 3. The knight's tour.

Example 4 (the magic five-pointed star). Show that it is impossible to place the numbers 1 through 10 on the ten intersection points of a five-pointed star (see Figure 4a) in such a way that each number is used exactly once, and the sum of the four numbers on any line in the star is the same.

[A magic six-pointed star is shown in Figure 4b.]

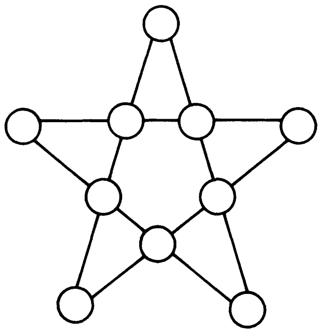


FIG. 4a. A five-pointed star. In a magic star, each number from 1 to 10 would be used exactly once, and the sum of the four numbers on every line in the star would be the same.

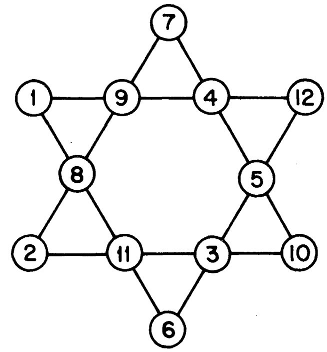


FIG. 4b. A six-pointed magic star.

Solutions to Examples 1, 2, 3, 4. *Solution to Example* 1 (the rook's tour of a chessboard). A hint is contained in the word "chessboard". You may have noticed that, in Figure 1 above, I didn't color the squares. If this were done (see Figure 5), then it would become clear that each move of our "rook-king" carries the piece from a white square to a black one or vice versa. Thus, to get from the starting point (a white square in Figure 5) to the finish (another white square), must involve an EVEN number of moves. However, the first square being occupied, there are 63 squares left to fill, an ODD number. Since the number of moves must, at the same time, be both odd and even, we have reached a contradiction, and the puzzle is impossible.

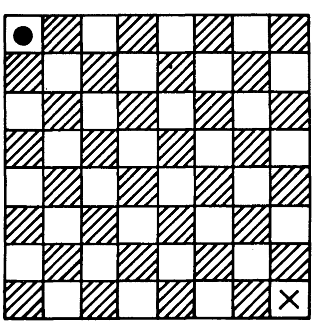


FIG. 5. The chessboard of the rook's tour with its squares colored in.

Solution to Example 2 (the 15-puzzle). Here we use the same idea as in Example 1, plus one new idea. Firstly, each time a "move" is made in the 15-puzzle, *the empty square moves vertically or horizontally*, just like the "rook-king" in Example 1 (here see Figure 6). Thus, for the same reason as before, it must require an EVEN number of moves to bring the empty square back to its original position. However, it can be shown that interchanging the

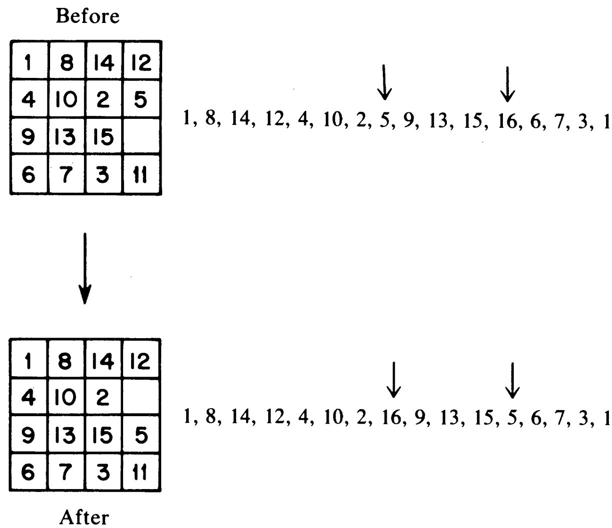


FIG. 6. A typical move in the 15-puzzle: the number 5 piece changes places with the empty square (which we consider to be square number 16). The *permutations* of 1, · · ·, 16 corresponding to these positions, are indicated to the right of the boxes.

14-piece with the 15-piece (if it could be done), would require an ODD number of moves. Thus we arrive at the same contradiction as in Example 1. The proof that the number of moves (if there were a solution) must be odd depends on some elementary facts about *permutations.* Since the theory of permutations is included in practically every textbook on group theory, linear algebra, or determinants (see, e.g., [3]), I will not attempt to outline it in this space. For those who know this theory, here is the proof that the number of moves in the 15-puzzle must be odd:

Let the empty square in the 15-puzzle be labeled "square number 16". Then any possible position of the fifteen pieces plus the empty square corresponds to a permutation of the integers 1 through 16 (where the natural ordering is, of course, defined to be that shown in Figure 2a above). Thus the positions shown in Figures 2a and 2b correspond respectively to the permutations:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16

and

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 14, 16

(note the inversion of 14 and 15 in the second case). The first permutation (the identity permutation) is even, and the second is odd. Now the theory of permutations tells us that to pass from an odd to an even permutation always requires an odd number of "moves" (where each "move" consists of exchanging two numbers, leaving the others fixed). In the 15-puzzle, each move amounts to an interchange of some piece with the empty square, number 16. This fits the situation required for permutation-theorem just cited, and shows that the number of moves must be odd.

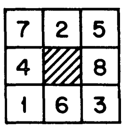


FIG. 7a. The cycle 1,2,3, · · ·, 8, 1 and its inverse show the only possible moves for a knight on this 3 by 3 board.

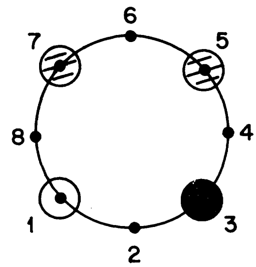


FIG. 7b. The circular representation. Here each point on the circle corresponds to the point labeled with the *same number* on the square. (Thus the point 2, at the bottom of the circle, corresponds to a point at the top of the square.) In this representation, the allowable moves are simply to go one space sideways around the circle.

Solution to Example 3 (the wandering knights). The square in the center of the 3×3 board is inaccessible to all of the knights. Number the remaining eight squares as shown in Figure 7a. Then the only possible moves for the knights are from square 1 to 2 to 3 to 4 to 5 to 6 to 7 to 8 to 1, and backwards (the inverses of the preceding moves). Thus we may represent the playing board by eight points situated on a circle (Figure 7b). In this *circular representation*, the allowable moves are simply to go one space clockwise or counterclockwise around the circle. In particular, since the pieces cannot occupy the same space and cannot capture, the pieces can never "jump" over one another. Now the invariant which solves the problem is seen to be topological: For, in order to interchange the positions of the black and white pieces, the two red pieces would have to be squeezed in between — i.e., the two red pieces would both end up occupying square number 2, which violates the rules.

[To make this argument precise, define the region "between" the black and white pieces to consist of all the positions on the circle traversed while moving in the *counterclockwise* direction *from* the black piece *to* the white one. Since the pieces can move only one space at a time (around the circle in Figure 7b), and cannot jump over one another, the two red pieces must remain "between" the black and the white one. Suppose, as required in the problem, the black piece moves to square number 1, and the white piece occupies square 3. Then the two red pieces must lie on squares "between" 1 and 3 (in the sense defined above); and the only such square is number 2.]

Solution to Example 4 (the magic star). We give a proof based on the idea that the set of numbers 1, · · ·, 10 is too small to allow the two "extreme" numbers 1 and 10 to be balanced by the more "moderate" numbers in between. Thus here, size rather than parity plays the crucial role. (For an alternative solution, based on considerations of odd and even, see [7].)

Step (i). If a solution were possible, the sum of the numbers in each line would be 22 (= 4 times the average 5.5 of the numbers 1 to 10). This is obvious.

Step (ii). If a solution existed, then the numbers 1 and 10 would have to lie on a single line.

Proof. Otherwise, take the six other numbers on the two lines passing through the point containing 1: These six numbers would have a sum $\leqq 9+8+7+6+5+4=39$. But by step (i), their sum must be $21+21=42$.

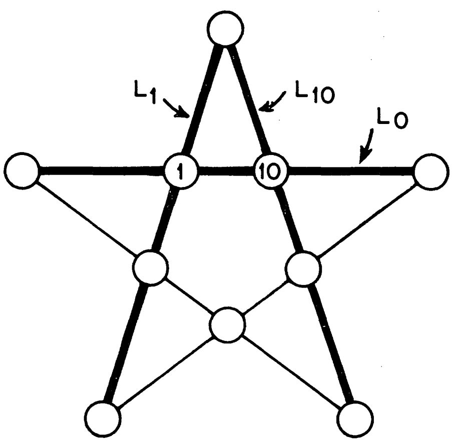


FIG. 8. A five-pointed star, with the numbers 1 and 10 placed on particular points, and the three lines L_0, L_1, and L_{10} indicated.

(Note: the proof which we give is independent of the actual location of the numbers 1 and 10; except that, after Step (ii), we know that 1 and 10 must lie on a single line.)

Note. Figure 8 is drawn just to give some sort of picture. It will NOT matter in the proof exactly *where* the numbers 1 and 10 lie on the star. The only fact that we need is that *any two lines in a five-pointed star intersect.*

Step (iii). Now assume that the numbers 1 and 10 are on a single line, which we call L_0 (see Figure 8). Call the two other lines through 1 and 10 respectively L_1 and L_{10}.

We must enumerate some possibilities; fortunately there are not very many. We list all of the possible combinations of numbers (1 and 10 are excluded) which could fill the *two empty spaces* on the line L_0 or the *three empty spaces* on the lines L_1 and L_{10}. (Recall that the sum of the four numbers along each line must be 22.) We go further: first we list all of the possibilities for L_0 (in the left hand column in Table 9); then *to the right of each L_0 entry, we list all of the L_1 and L_{10} combinations which are compatible with it.*

In L_0	In L_1	In L_{10}
(Besides 1, 10)	(besides 1)	(besides 10)
9,2	8,7,6	3,4,5
8,3	9,7,5	2,4,6
7,4	none	none
6,5	9,8,4	2,3,7

TABLE 9. Possible sets of numbers to fill the vacant spaces on the lines L_0, L_1, and L_{10} in Figure 8. The sum of the four numbers along each line must be 22.

Thus, in the first case given in Table 9, the lines L_0, L_1, and L_{10} would contain the following sets of four numbers:

$$L_0=\{1,\ 10,\ 9,\ 2\},\qquad L_1=\{1,\ 8,\ 7,\ 6\},\qquad L_{10}=\{10,\ 3,\ 4,\ 5\}.$$

Finally, we recall the fact that any two lines in a five-pointed star intersect. However, in each of the possibilities listed in Table 9, the lines L_1 and L_{10} have no common element. This contradiction proves the impossibility of constructing a five-pointed magic star.

Discussion. What invariants have been used so far? The idea of odd and even, obviously, in Examples 1 and 2; the topological notion of "betweenness" in Example 3, and the limitations forced by the sizes of the numbers in Example 4. There are also, in each problem, constructs (i.e., "tricks") designed to bring these invariants into play. Thus we have:

The operation of coloring the squares of the chessboard, in Example 1.

The idea of odd and even permutations, and the proposition that it requires an odd number of moves to turn one into the other, in Example 2.

The trick of turning the "knight's walk" around the tic-tac-toe board into a circular motion, in Example 3.

The method of looking at the two "extreme" numbers 1 and 10, in Example 4. There we also used the fact that any two lines in a five-pointed star intersect, which illustrates another kind of invariant.

In the problems which follow, based on Galois theory, the invariants are more complicated. As already stated, here we cannot give the details. We will attempt, in discussing these problems, to make comments which may be suggestive to a reader who does not know Galois theory, and (hopefully) clear to a reader who does.

Examples depending on Galois theory. *Example* 5 (trisection of an angle). The problem of deciding whether it is possible, using the "classical" instruments of Greek geometry, the straightedge and compass, to trisect an arbitrary angle, remained an open mathematical question for about two thousand years. It was finally settled around the year 1800, when it was proved that the construction is impossible. (Incidentally, this result seems to have the status of a "folk-theorem" — at least it is not generally attributed to any one man. It was certainly implicit in the work of Gauss, but may have been known earlier.)

Paul Erdös, in an offhand lecture given at the University of Minnesota, made some interesting comments on problems which remain untouched for hundreds of years. He remarked (the quote is a rough one, of course):

"Archimedes knew the impossibility of trisecting an angle. But he also knew that proving this proposition was not for his time, and so he concentrated his energies on problems that he could solve."

If so, Archimedes' judgment was sound, for at present, all known approaches to the trisection problem involve ideas from the so-called "modern algebra", a subject not highly developed until the eighteenth century. Indeed, it appears that the trisection problem really has very little to do with "geometry". In its solution, the geometric problem is immediately translated into a problem in algebra. We may outline the steps in the solution as follows:

[Here I will make free use of the language of contemporary algebra — hopefully this will convey something of the flavor of the argument, even to nonspecialists.]

(1) The geometric problem is translated into a problem about numbers, using the sort of analytic geometry that is familiar to every calculus student today.

(2) Each straightedge and compass construction generates certain points; these points have coordinates (via analytic geometry), and so they generate in turn a certain set of numbers.

(3) These numbers (here is where the terminology gets thick) lie in what is called a "number field", which is an extension of the field of rational numbers. This number field is then viewed as a "vector space" over the subfield of rationals. *This allows us to speak of the DIMENSION of that vector space, which becomes an invariant arising out of the geometrical construction.*

(4) It is shown that the "dimension" of these vector spaces over the rationals is always *a power of two.*

[*Note.* The dimension need NOT be two; it can be $2, 4, 8, 16, \cdots$. This corresponds to the fact that straightedge and compass constructions can be very complex. Such complexity would be reflected in the fact that the resulting number fields had very high dimension over the rationals. Here recall our earlier question: "How do we know that there is not some intricate construction, involving perhaps thousands of steps, which our proof has overlooked?"]

(5) We have seen that straightedge and compass constructions give number fields whose dimension over the rationals must be a power of two. Now it turns out that, to trisect most angles, one requires number fields whose dimension is three, or a multiple of three. Since no power of two is ever, at the same time, a multiple of three, we have reached an impasse. Thus the assumption that it is possible, using the "classical instruments", to trisect an arbitrary angle, leads to a contradiction.

Remark. The reader might ask: Why use only the "classical instruments", the straightedge and compass? One answer is that it makes a good problem! Another answer is that those instruments are, after all, the simplest ones; both of them can be bought for under a dollar. (How much longer will this remain true?)

There are many other drawing instruments, of course. For a good discussion of these, I recommend the books of Felix Klein [**6**] and Howard Eves [**4**]. Eves' book stresses the geometric aspects; Klein's book, the algebraic and analytic. Klein's book, incidentally, contains proofs of the impossibility of trisecting the angle, duplicating the cube, and squaring the circle.

Note. Like all "impossibility theorems", the one about trisecting angles is valid only if carefully formulated. Thus, the only instruments allowed are the straightedge (a ruler without markings) and the compass. Furthermore, an *exact* construction is required. (Approximate constructions abound.)

[Someone called the author once, and announced that he thought he had found a method for trisecting angles. However, he said, he had forgotten his high school trigonometry, and wondered whether I would be willing to do some calculations for him. When I informed him about the impossibility theorem, I expected some disagreement. Instead, the conversation ended on a rather surprising note. Evidently the fellow was much impressed by my abilities, for he asked me: "Say, this probably isn't your department, but do you know anything about mushrooms?" Unfortunately, I couldn't help him there.]

Example 6 (linear combinations of *n*th roots). The last two examples will be treated only very briefly. The reason for including them at all is that they follow, with increasing levels of sophistication, the pattern set by the trisection problem (Example 5).

[In technical language: the trisection problem involves only the idea of the *dimension* of a vector space. Example 6, when treated via Galois theory, requires somewhat more: the *noncommutativity* of a certain group. (For a discussion of how this comes about, cf. [**8**].) Finally, the classic problem of the quintic equation in Example 7, involves the full apparatus of Galois theory.]

Now to come to the question: Every student of mathematics learns the result that *n*th roots of integers, such as $\sqrt{2}$ or $\sqrt[3]{4}$, are irrational except in the trivial cases (like $\sqrt{4}$) when they reduce to whole numbers. A much more difficult problem is to treat *linear combinations* of *n*th roots, e.g.:

$$\sqrt[4]{3}+\sqrt[5]{4}+\sqrt[6]{72}. \tag{E}$$

However, the result which one expects to be true does hold: Sums such as (E) are irrational whenever their terms do not "obviously" cancel out. It is not difficult to formulate this statement precisely; the technical version is as follows:

In the first place, by the "*n*th root" of a positive integer, we mean here the real positive *n*th root. Now, for simplicity, we will state a special case of our theorem, involving 60th roots of integers whose only prime factors are 2 and 3.

The reader who wishes to, will find no difficulty in devising a suitable generalization.

THEOREM. *Consider the set of positive real numbers*:

$$\sqrt[60]{2^a 3^b}, \qquad 0 \leqq a < 60, \qquad 0 \leqq b < 60.$$

These 3600 *numbers are linearly independent over the rational field.*

Remarks. The reader may be wondering what the above theorem has to do with "impossibility". To see the connection, let us take the four real numbers:

$$1, \quad \sqrt[4]{3}, \quad \sqrt[5]{4}, \quad \sqrt[6]{72}.$$

These form a subset of the set of 3600 numbers mentioned in the theorem. To say that they are "linearly independent over the rationals" means that it is impossible to find rational numbers a, b, c, d, not all zero, such that

$$a + b\sqrt[4]{3} + c\sqrt[5]{4} + d\sqrt[6]{72} = 0.$$

(This, incidentally, shows that the number exhibited in (E) above is irrational.)

As I have said, the theorem is expected; much more surprising is the fact that it has, apparently, no elementary proof. (If one is content to consider only square-roots, and ignore cube-roots and higher radicals, then there are elementary solutions; see e.g., [**5**].) The theorem in its general form was first proved by Besicovitch [**2**]. A treatment based on Galois theory has been given by the author [**8**]. For extensions to number fields other than the rationals, see the paper of Siegel [**9**], and a paper by Schinzel to appear in Acta Arithmetica.

Example 7 (the quintic equation). As every student of high school algebra knows, there is a simple formula for solving the general quadratic equation:

$$\text{if } ax^2 + bx + c = 0, \quad \text{then} \quad x = [-b \pm \sqrt{b^2 - 4ac}]/2a.$$

This formula involves, besides the rational operations (addition, subtraction, multiplication, and division), only the square-root. There are similar, but much more complicated, formulas for solving 3rd degree and 4th degree polynomial equations. Then, abruptly, the situation changes: there is no formula involving radicals (nth roots) for solving the general 5th degree equation.

Like many such results, this one was certainly suspected before it was proved. Important contributions were made by Lagrange, Gauss, Cauchy, Ruffini, Abel, and Galois. The approach used by Galois was the most far-reaching, and (having been, by now, greatly simplified) it is commonly taught in university courses in algebra today.

Unfortunately, such results are not accessible to anyone except a mathematical specialist. For teaching purposes, the puzzles given in Examples 1 to 4 above, may provide a reasonable introduction to this kind of mathematical thought. At least, the simple arguments which we gave there possess the essential ingredients of a mathematical proof — they are completely convincing!

To return to the children's platitude cited at the beginning of this article: "While one man was proving it couldn't be done, another man tried and he did it." If anyone does something which has *really* been proved to be impossible, then you may be sure that he cheated a little.

Added in Proof. William Pruitt has shown me a simplified proof for the magic five-pointed star (Example 4) which eliminates completely the "enumeration of cases" required in my solution. He follows my proof through Step (ii), in which it is shown that, if a magic five-pointed star did exist, then the numbers 1 and 10 would have to lie on the same line (again call it L_0). However, here he makes the following pretty observation: Step (iii*): *If a magic star did exist, then on no line in the star would there be two numbers whose sum is* 11. Clearly (iii*) contradicts (ii)!!!

Proof of (iii*). Suppose such a line, call it L_0, did exist with four numbers u, $11-u$, v, $11-v$ on it. Let L_1, L_2, L_3, L_4 be the other four lines in the star, passing through the numbers u, $11-u$, v, $11-v$ respectively. (Here a glance at Figure 8 above may be helpful.) Consider the lines L_1 and L_2 as being "+" and the lines L_3 and L_4 as being "−". Then the algebraic sum of the numbers in these lines, counted according to multiplicity, and weighted with the "+" or "−" signs as indicated, would be $22+22-22-22=0$. Now let x be the number through which the pair of lines L_1 and L_2 intersect; similarly define y with reference to L_3 and L_4. We leave it to the reader to verify: The above "algebraic sum" $=0=u+(11-u)-v-(11-v)+2x-2y$ (all of the other numbers cancel out with one "+" sign and one "−" sign). Hence $2x-2y=0$, and $x=y$, a contradiction.

The author wishes to thank Mike Lutter for his valuable criticism of the first part of this manuscript.

References

1. E. Artin, Galois theory (with a section on applications by A. N. Milgram), Notre Dame Mathematical Lectures no. 2, 1942.

2. A. S. Besicovitch, On the linear independence of fractional powers of integers, J. London Math. Soc., 15 (1940) 3–6.

3. G. Birkhoff and S. MacLane, A Survey of Modern Algebra, rev. ed., Macmillan, New York, 1965.

4. H. Eves, A Survey of Geometry, rev. ed., Allyn and Bacon, Boston, 1972.

5. H. Flanders, (Solution of a problem posed by D. J. Newman), Amer. Math. Monthly, 67 (1960) 188–189.

6. F. Klein, Famous Problems of Elementary Geometry, repr. by Dover, New York, 1956.

7. H. Langman, Play Mathematics, Hafner, New York, 1962.

8. I. Richards, An application of Galois theory to elementary arithmetic, Advances in Math., 13 (1974) 268–273.

9. C. L. Siegel, Algebraische Abhängigkeit von Wurzeln, Acta Arith., 21 (1972) 59–64.

10. B. L. van der Waerden, Algebra, vol. 1, rev. ed., Ungar, New York, 1970.

ON THE NUMBER OF PRIME FACTORS OF A PAIR OF RELATIVELY PRIME AMICABLE NUMBERS

PETER HAGIS, JR., Temple University

1. Introduction. The natural numbers m and n are said to be amicable if

(1) $$\sigma(m) = \sigma(n) = m + n$$

where, as usual, $\sigma(k)$ denotes the sum of the positive divisors of k. None of the approximately 1100 pairs of amicable numbers which have been discovered to date (see [**6**] for an *almost* complete list of known amicable numbers) is relatively prime (for three is a common factor of every known *odd* amicable pair while no amicable pair of opposite parity has as yet been found). Indeed, whether or not a relatively prime amicable pair exists is still very much an open question. In 1953 Kanold [**4**] showed that the product of a pair of relatively prime amicable numbers must be divisible by at least twenty-one different primes. Our purpose here is to improve Kanold's result as follows:

THEOREM. *If m and n are relatively prime amicable numbers, then mn is divisible by at least twenty-two different primes.*

The author has already proved the following proposition in an earlier paper [**3**].

PROPOSITION 1. *If m and n are relatively prime odd amicable numbers, then mn has at least twenty-two prime factors.*

Thus, our theorem will follow *if* we can establish the following result:

PROPOSITION 2. *If m and n are relatively prime amicable numbers of opposite parity, then mn has at least twenty-two prime factors.*

The rest of this paper is devoted to a proof of this proposition.

2. Some preliminaries. We assume that m and n are amicable numbers (so that (1) holds) such that $(m, n) = 1$ and m is even. It is proved in [**2**] (see also [**5**]) that

(2) $$m = 2M^2, \quad n = N^2 \text{ where } (6, MN) = 1.$$

By a theorem due to Euler (see page 3 in [**1**]), if $(x, y) = 1$ and y is odd, then every prime factor of $2x^2 + y^2$ is of the form $8k + 1$ or $8k + 3$. From (1), (2) and the multiplicative property of $\sigma(n)$, we have:

LEMMA 1. *If* $p^\alpha \| mn$ *and* $q \mid \sigma(p^\alpha)$, *then* $q \equiv 1,3 \pmod 8$.

Here, and in the sequel, p and q are odd primes. $p^\alpha \| k$ means that $p^\alpha \mid k$ but $p^{\alpha+1} \nmid k$.

Now we know from Kanold [4] that mn has *at least* twenty-one prime factors. Therefore, Proposition 2 will be proved *if* we can demonstrate that mn cannot have *exactly* twenty-one prime divisors. Thus, from now on, and without further mention, we assume that mn is divisible by exactly twenty-one primes. This assumption will prove to be untenable.

The proof of our next lemma may be found in [**3**].

LEMMA 2. *mn is divisible by each of the sixteen primes p such that* $5 \leqq p \leqq 61$ *and by at most one prime greater than* 83. *If Q is the largest prime which divides mn, then* $Q \leqq 113$.

REMARK 1. From (2), $3 \nmid mn$.

We shall also require some facts concerning cyclotomic polynomials. If $F_k(x)$ denotes the cyclotomic polynomial of order k, then according to Theorem 3.4 in [**8**]

$$\sigma(p^\alpha) = (p^{\alpha+1} - 1)/(p - 1) = \prod_d F_d(p) \text{ where } d > 1 \text{ and } d \mid (\alpha + 1). \tag{3}$$

REMARK 2. It follows from (3) that if $k \mid (\alpha + 1)$ and $e \mid k$ where $e > 1$, then $F_e(p) \mid \sigma(p^\alpha)$. Of course, if $p^\alpha \| n$, then $F_e(p) \mid \sigma(n)$ also.

The following lemma is a consequence of Theorems 94 and 95 in [**7**], but we include its proof for the sake of completeness. $E(p;q)$ denotes the exponent to which p belongs modulo q. (For a discussion of "belonging to an exponent" see Section 2.9 in [**9**].)

LEMMA 3. *Let* $h = E(p; q)$. *If* $q \mid F_k(p)$, *then* $h \mid k$. *If* $h < k$, *then* $q \mid k$.

PROOF. Since $q \mid F_k(p)$ we see from (3) that $q \mid (p^k - 1)$ so that $h \mid k$. If $k = hr$ where $r > 1$, then

$$(p^k - 1)/(p^h - 1) = (p^{hr} - 1)/(p^h - 1) = 1 + p^h + p^{2h} + \cdots + p^{(r-1)h}.$$

Since $p^h \equiv 1 \pmod q$, and $q \mid F_k(p)$, and $F_k(p) \mid (p^k - 1)/(p^h - 1)$ (again using (3)), it follows that $0 \equiv r \pmod q$. Thus, $q \mid k$.

COROLLARY 3.1. *If* $3 \mid F_k(p)$ *where k is odd and different from one, then* $3 \mid k$ *and* $p \equiv 1 \pmod 3$ $(E(p; 3) = 1)$.

3. **The plan**. We are now prepared to attack Proposition 2. First an explanation of our strategy. From (1), (2), (3) and the multiplicative property of the sigma function, it follows that if $q \mid \sigma(m)$, then there exist integers k and α (both greater than one) and an odd prime p such that $p^\alpha \mid\mid n$ and $q \mid F_k(p)$, where k is a divisor of $\alpha + 1$. Since α is even we see that k is odd. Candidates for p and k may be found by imposing the restrictions given in Lemmas 2 and 3. In particular, we see that p is not *acceptable* if E(p; q) is even. It now follows from (1) that, since $F_k(p) \mid \sigma(p^\alpha)$, *both* $\sigma(n)$ and $\sigma(m)$ are divisible by $F_k(p)$ *and* by $F_e(p)$ if $e \mid k$ and $e > 1$ (recall Remark 2). We shall take e to be a divisor of $E(p; q)$ in most cases.

We shall proceed in two stages. At each stage we show that $\sigma(m)$ or $\sigma(n)$ must be divisible by at least one element from a well-defined finite set of primes. In consequence of the preceding discussion $\sigma(m)$ and $\sigma(n)$ must be divisible by a cyclotomic number (or numbers), say $F_e(p)$. Of course, $p \mid mn$. If $q \mid F_e(p)$ and $5 \leqq q \leqq 61$, then (1), Lemma 2 and the fact that $(m, n) = 1$ yield an immediate contradiction which we will characterize as being of TYPE A. We also have a contradiction, according to Lemma 1, if $q \mid F_e(p)$ and $q \equiv 5, 7 \pmod 8$. We will identify these as being of TYPE B. If no contradiction arises the factors of $F_e(p)$ furnish possible starting points for the next stage. In the final stage all possibilities yield contradictions, thus completing our proof by *reductio ad absurdum*.

It will become clear that Lemma 3 is an indispensable tool in our procedure. The pertinent values of $E(p; q)$ and the factors of $F_e(p)$ were found with the aid of the CDC 6400 at the Temple University Computing Center.

4. **Stage I.** We show first that $\sigma(m)$ is divisible by at least one of the four primes 331, 1801, 3169 or 3571. Since $\sigma(2) = 3$ we see from (2) that $3 \mid \sigma(m)$. From our discussion in Section 3, n has at least one prime power divisor p^α such that $3 \mid F_k(p)$ where k is odd and $k \mid (\alpha + 1)$. From Corollary 3.1 and Remark 2, $p \equiv 1 \pmod 3$ and $F_3(p) \mid \sigma(m)$. From Lemma 2 the possible values of p are 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109. But $7 \mid F_3(p)$ if $p = 37, 67, 79, 109$; $13 \mid F_3(7)$; $61 \mid F_3(13)$ so that these cases yield contradictions of TYPE A. Contradictions of TYPE B arise if $p = 19$ or 43. For $127 \mid F_3(19)$ and $631 \mid F_3(43)$. Thus, $F_3(31) = 3 \cdot 331 \mid \sigma(m)$ or $F_3(73) = 3 \cdot 1801 \mid \sigma(m)$ or $F_3(97) = 3 \cdot 3169 \mid \sigma(m)$ or $F_3(103) = 3 \cdot 3571 \mid \sigma(m)$.

5. **Stage II.** Suppose that $1801 \mid \sigma(m)$ and $73 \mid n$. Then m has a prime factor $p \neq 73$ such that $1801 \mid F_k(p)$ where k is odd. But this is impossible by Lemma 3, since a computer search showed that $E(p; 1801)$ is even if $5 \leqq p \leqq 113$ and $p \neq 73$.

If $97 \mid n$ and $3169 \mid \sigma(m)$ then, by Lemma 2, m has no prime divisors greater than 83. Since $E(13; 3169) = 99$ and $E(p; 3169)$ is even for $p \leqq 83$ and $p \neq 13$, we conclude from Lemma 3 and Remark 2 that $F_3(13)|\sigma(m)$. Since $61|F_3(13)$ we have a contradiction of TYPE A.

Now suppose that $31|n$ and $331|\sigma(m)$. Calculating $E(p; 331)$ for $p \neq 31$ and $5 \leqq p \leqq 113$ we find it is even except in the following cases:

$E(83; 331) = 15$, $E(p; 331) = 33$ if $p = 79$ or 89; $E(67; 331) = 55$; $E(p; 331) = 165$ if $p = 5, 17, 19, 43, 53, 71, 103, 109, 113$. From Lemma 3 and Remark 2 $F_e(p)|\sigma(m)$ where p is one of these *acceptable* primes and $e|E(p; 331)$. But $5|F_5(71)$; $7|F_3(p)$ if $p = 53, 79, 109$; $11|F_{11}(p)$ if $p = 67, 89$; $11|F_5(103)$; $13|F_3(113)$; $19|F_3(83)$; $31|F_3(5)$ yielding TYPE A contradictions. $F_5(17) = 88741 \equiv 5 \pmod 8$; $127|F_3(19)$, $631|F_3(43)$ and $127 \equiv 631 \equiv 7 \pmod 8$ so that these three possibilities yield contradictions of TYPE B.

The only remaining possibility is that $103|n$ and $3571|\sigma(m)$. By Lemma 2, m has no prime factor greater than 83. If $5 \leqq p \leqq 83$ then $E(p; 3571)$ is even except for the following: $E(47; 3571) = 17$, $E(p; 3571) = 119$ if $p = 17$ or 59; $E(p; 3571) = 225$ if $p = 41$ or 71; $E(p; 3571) = 357$ if $p = 43$ or 67; $E(p; 3571) = 1785$ if $p = 5, 11, 13, 19, 29, 31, 73, 83$. Reasoning as before, if $e|E(p; 3571)$ then $F_e(p)|\sigma(m)$ for at least one of these fifteen values of p. But ten of them lead to TYPE A contradictions and five to TYPE B contradictions. For $5|F_5(p)$ if $p = 11, 31, 41, 71$; $13|F_3(29)$; $19|F_3(83)$; $31|F_3(p)$ if $p = 5, 67$; $43|F_7(59)$; $61|F_3(13)$. Also, $F_7(17) = 25646167 \equiv 7 \pmod 8$; $F_5(73) = 28792661 \equiv 5 \pmod 8$; $127|F_3(19)$, $631|F_3(43)$, $2127357527|F_{17}(47)$ and $127 \equiv 631 \equiv 2127357527 \equiv 7$ (mod 8). We have reached an impasse which establishes the truth of Proposition 2 and our theorem.

Acknowledgement. The discovery that the prime 2127357527 is a factor of $F_{17}(47)$ is due to D.H. Lehmer.

References

1. L. E. Dickson, History of the Theory of Numbers, vol. 3, Chelsea, New York, 1966.

2. P. Hagis, Jr., Relatively prime amicable numbers of opposite parity, this Magazine, 43 (1970) 14–20.

3. ———, Relatively prime amicable numbers with twenty-one prime divisors, this Magazine, 45 (1972) 21–26.

4. H.-J. Kanold Untere Schranken für teilerfremde befreundete Zahlen, Arch. Math., 4 (1953) 399–401.

5. ———, Über befreudete Zahlen II, Math. Nachr., 10 (1953) 99–111.

6a. E. J. Lee and J. S. Madachy, The history and discovery of amicable numbers — Part 1, J. Recr. Math., 5 (1972) 77–93.

6b. ———, The history and discovery of amicable numbers — Part 2, J. Recr. Math., 5 (1972) 153–173.

6c. ———, The history and discovery of amicable numbers — Part 3, J. Recr. Math., 5 (1972) 231–249.

7. T. Nagell, Introduction to Number Theory, Wiley, New York, 1951.

8. I. Niven, Irrational Numbers, Wiley, New York, 1956.

9. I. Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, 3rd. ed., Wiley, New York, 1972.

A CHARACTERIZATION OF CONDITIONAL PROBABILITY

PAUL TELLER and ARTHUR FINE, University of Illinois at Chicago Circle

1. Let $\langle X, \mathscr{F}, P\rangle$ be a probability space; that is, suppose that X is a nonempty set, that $\mathscr{F}$ is a field of subsets of X and that P is a nonnegative, additive measure on $\mathscr{F}$ satisfying $P(X) = 1$. (The measure may be finitely or countably additive.) If B is an $\mathscr{F}$-measurable subset of X with nonzero probability, then the measure $P(\cdot\,/B)$ for conditional probability relative to B satisfies these two conditions:

(1.1) $P(B/B) = 1$ and

(1.2) there is a function g such that for all $\mathscr{F}$-measurable subsets A of B, $P(A/B) = g[P(A)]$ (namely, $g(x) = x/P(B)$).

The purpose of this note is to show that if there are enough probabilities in the space then these two conditions characterize conditional probability.

2. By "enough probabilities" we mean that the space is *full*, in the sense of the following definition:

DEFINITION 1. *The space* $\langle X, \mathscr{F}, P\rangle$ *is full* (see [**2**]) *iff* P *maps the* $\mathscr{F}$*-measurable subsets of any* $B \in \mathscr{F}$ *onto the interval* $[0, P(B)]$.

Fullness implies that if $0 \leqq x \leqq y \leqq x + y \leqq P(B)$, then there are disjoint subsets C, D of B satisfying $P(C) = x$ and $P(D) = y$. For we can find $C \subseteq B$ so that $P(C) = x$. But then $P(B - C) = P(B) - x$. Since $y \leqq P(B) - x$ we can use the fullness again to find $D \subseteq (B - C)$ so that $P(D) = y$.

The proof of the characterization makes use of a nice property of additive functions which is formulated in the following lemma:

LEMMA. *The only nonnegative, additive function g on the interval* $[0, b]$ *is the function* $g(x) = kx$ *where* $k = g(b)/b$.

Proof. (Due to Darboux, 1880; see [**1**], p. 32 ff., see also [**3**].) If g is nonnegative and additive on $[0, b]$, then g is order preserving, since if $0 \leqq x < y \leqq b$, then $y = x + z$ for some $z \in [0, b]$ and so $g(y) = g(x) + g(z) \geqq g(x)$. Since $g(0) = g(0 + 0) = 2g(0)$, one has that $g(0) = 0$. Also $g(b) = (g(b)/b)\cdot b = kb$. So $g(x) = kx$ for $x = 0, b$. The rational multiples $(n/m)b$ of b in $[0, b]$ are dense in the interval. They too satisfy $g(x) = kx$. For

$$g(b) = g\left(\frac{b}{m}\right) + \overset{m\text{-times}}{\cdots} + g\left(\frac{b}{m}\right) = mg\left(\frac{b}{m}\right).$$

Hence,

$$g\left(\frac{nb}{m}\right) = n\cdot g\left(\frac{b}{m}\right) = n\cdot\frac{g(b)}{m} = k\cdot\frac{nb}{m}.$$

Consider, finally, any $x \in (0, b)$. There are sequences $\{u_n\}$ and $\{v_n\}$ of rational multiples of b in $[0, b]$ that converge to x, so that for each n

$$u_n \leqq x \leqq v_n.$$

Since g is order preserving,

$$g(u_n) \leqq g(x) \leqq g(v_n).$$

Since $g(u_n) = k \cdot u_n$ and $g(v_n) = k \cdot v_n$, it follows that $g(x) = kx$.

We now characterize conditional probability in the following theorem:

THEOREM 1. *Let $\langle X, \mathcal{F}, P \rangle$ be a full probability space. Suppose $P(B) \neq 0$ and let P' be a measure on the space. Then the following conditions are both necessary and sufficient for $P' = P(\cdot / B)$:*

(2.1) $P'(B) = 1$ *and*

(2.2) *for all $\mathcal{F}$-measurable subsets A, A' of B, if $P(A) = P(A')$, then $P'(A) = P'(A')$.*

Proof. Since $P(A/B) = P(A \cap B)/P(B)$, the necessity is straightforward. To prove sufficiency, notice first that condition (2.2) is just another way of asserting that the pairs $\langle P(A), P'(A) \rangle$ constitute a function g, satisfying $g[P(A)] = P'(A)$ for all $\mathcal{F}$-measurable subsets A of B, as in (1.2). By fullness this function g is defined on $[0, P(B)]$. It is nonnegative. We can show that it is additive as follows. Consider x, y satisfying $0 \leqq x \leqq y \leqq x + y \leqq P(B)$. By the fullness of the space there are disjoint subsets C, D of B such that $P(C) = x$ and $P(D) = y$. Then

$$g(x+y) = g[P(C) + P(D)] = g[P(C \cup D)] = P'(C \cup D) = P'(C) + P'(D)$$
$$= g[P(C)] + g[P(D)] = g(x) + g(y).$$

It follows from the lemma that $g(x) = kx$, where $k = g[P(B)]/P(B)$. But $g[P(B)] = P'(B) = 1$, by (2.1). Hence for any $\mathcal{F}$-measurable subset S of B, $P'(S) = P(S)/P(B)$. Finally, if A is any $\mathcal{F}$-measurable set, then

$$P'(A) = P'(A \cap B) + P'(A \cap \bar{B}).$$

Since $P'(B) = 1$, $P'(\bar{B}) = P'(A \cap \bar{B}) = 0$. Since $(A \cap B) \subseteq B$ we have that

$$P'(A) = P'(A \cap B) = \frac{P(A \cap B)}{P(B)} = P(A/B).$$

3. This theorem characterizes conditional probability as the only renormalized measure (Condition (2.1)) that is functionally related (Condition (2.2)) to the original measure on the space. It is important to realize that this characterization leans heavily on the fullness of the space. If the space is not full, then these conditions will not single out conditional probability. The following simple example shows this:

Let $X = \{x_1, x_2, x_3\}$, let $\mathcal{F} = 2^X$ and let P be determined by $P(x_1) = 1/8$, $P(x_2) = 3/8$ and $P(x_3) = 4/8$. If P' is defined by $P'(x_2) = 3/8$ and $P'(x_3) = 5/8$, then $P'(B) = 1$ where $B = \{x_2, x_3\}$ (and $P(B) = 7/8 \neq 0$). The function

$$g = \{\langle 0, 0\rangle, \langle 3/8, 3/8\rangle, \langle 4/8, 5/8\rangle, \langle 7/8, 1\rangle\}$$

defined on $\{0, 3/8, 4/8, 7/8\}$ connects P' to P according to the formula

$$P'(A) = g[P(A)] \quad \text{for all} \quad A \subseteq B.$$

Hence (2.1) and (2.2) are satisfied. Moreover g is one-one, monotone and even additive on its domain. Yet $P' \neq P(\cdot/B)$.

The juxtaposition of this example with Theorem 1 raises the question of what conditions on nonfull spaces might single out conditional probability. We state two results that bear on this question. The first, Corollary 1, is prompted by the fact that any space can be embedded in a full space and the corollary merely states obvious conditions on an embedding. The second result, Theorem 2, gives conditions weaker than fullness under which a sandwich argument similar to that of the lemma can be applied.

COROLLARY 1. *Necessary and sufficient for* $P' = P(\cdot/B)$ *is that* $P'(B) = 1$ *and that the space can be embedded into a full space* $\langle X^*, \mathcal{F}^*, P^*\rangle$ *in satisfaction of*

(3.1) *P^* extends P, and*

(3.2) *there is a measure P'^* on the full space that extends P' and which is such that for all $\mathcal{F}^*$-measurable subsets A, A' of B if $P^*(A) = P^*(A')$, then $P'^*(A) = P'^*(A')$.*

DEFINITION 2. *The space* $\langle X, \mathcal{F}, P\rangle$ *is full enough at* B *where* B *is an* $\mathcal{F}$*-measurable subset of* X *with* $P(B) \neq 0$, *iff*

(3.3) *C is an $\mathcal{F}$-measurable subset of B and $P(C) = (m/n)P(B)$, for integers m, n (in lowest terms), then there are n $\mathcal{F}$-measurable subsets that partition B, $X_1 \cdots X_i \cdots X_n$, such that $P(X_i) = P(X_j)$ for $1 \leqq i < j \leqq n$; and*

(3.4) *C is an $\mathcal{F}$-measurable subset of B and $P(C) = r\, P(B)$, r an irrational number, then there are four infinite sequences of $\mathcal{F}$-measurable subsets of B, $\{X_i\}$, $\{X'_i\}$, $\{Y_i\}$, $\{Y'_i\}$, such that the following conditions hold:*

(3.4a) *$P(X_i) \to P(C)$ from below and $P(Y_i) \to P(C)$ from above and for all i,*

(3.4b) *$P(X_i)$ and $P(Y_i)$ are rational multiples of $P(B)$, and*

(3.4c) *$P(X_i \cup X'_i) = P(C) = P(Y_i - Y'_i)$.*

THEOREM 2. *If the space* $\langle X, \mathscr{F}, P\rangle$ *is full enough at* B, *then conditions* (2.1) *and* (2.2) *of Theorem* 1 *are again necessary and sufficient for* $P' = P(\cdot/B)$.

As in Theorem 1, it follows from condition (2.2) that there is a function g satisfying $g[P(A)] = P'(A)$, except that g is defined only on the set $I = \{P(A) \mid A$ is an $\mathscr{F}$-measurable subset of $B\}$. It suffices to show that, where defined,

$$g(x) = kx, \qquad k = \frac{g[P(B)]}{P(B)}. \tag{3.5}$$

From (3.3) of Definition (2) it is easily shown that g is additive on all elements of I which are rational multiples of $P(B)$. If C is an $\mathscr{F}$-measurable subset of B such that $P(C) = (n/m)P(B)$, it follows, just as in the lemma, that $g[P(C)] = g[(n/m)P(B)] = (n/m)g[P(B)] = k\,P(C)$. If C is an $\mathscr{F}$-measurable subset of B such that $P(C) = r\,P(B)$ (r irrational) then, for all i,

(3.6) $P(X_i \cup X'_i) = P(C) = P(Y_i - Y'_i)$ by (3.4c) of Definition 2.

So

(3.7) $g[P(X_i \cup X'_i)] = g[P(C)] = g[P(Y_i - Y'_i]$ by assumption (2.2) of the theorem.

Also

(3.8) $g[P(X_i \cup X'_i)] = g[P(X_i)] + g[P(\bar{X}_i \cap X'_i)]$, and $g[P(Y_i - Y'_i)] = g[P(Y_i)] - g[P(Y_i \cap Y'_i)]$ follow from the assumption of (3.4) that all the relevant sets are $\mathscr{F}$-measurable subsets of B, in the same way that the general additivity of g is shown in Theorem 1.

Equations (3.8) and (3.7) give

$$g[P(X_i)] \leqq g[P(C)] \leqq g[P(Y_i)].$$

Since we have shown (3.5) for x which are rational multiples of $P(B)$, and since by (3.4b) of definition 2, $P(X_i)$ and $P(Y_i)$ are rational multiples of $P(B)$, we have

$$k\,P(X_i) \leqq g[P(C)] \leqq k\,P(Y_i). \tag{3.9}$$

Finally (3.9) and (3.4a) give

$$g[P(C)] = k\,P(C).$$

Abstract presented to the American Mathematical Society, January 17, 1974.

References

1. J. Aczél, Lectures on Functional Equations And Their Applications, Academic Press, New York, 1966.

2. Bas van Fraassen, Notes on probabilities of conditionals, (preprint, 1973).

3. G. S. Young, The linear functional equation, Amer. Math. Monthly, 65 (1958) 37–38.

MONOCHROMATIC LINES IN THE PLANE

DARYL TINGLEY, Dalhousie University

A theorem of T. S. Motzkin, which was first presented by him in a Colloquium talk at Dalhousie University in 1967, states that given two finite disjoint sets R and B in E^2 (the plane), with $R \cup B$ not a subset of any line, there is a line which contains two points of one of the sets, and is disjoint from the others. To make the problem easier to visualize we color the sets — say red for R and blue for B, and for obvious reaons we call the desired line *monochromatic*.

The above theorem is reminiscent of the famous Sylvester question concerning the existence, for a finite noncollinear set of points, of a line containing exactly two points of the sets.

The Sylvester problem has led to a number of related results in which the points of the original version were replaced by sets of points. One of the first such results was by B. Grünbaum [**1**] who proved that for any finite collection of two or more disjoint connected compact sets in E^2, whose union is not contained in a line, there is always a line intersecting exactly two members of the collection. We will prove that a similar result is true when the two finite sets in the Motzkin Theorem are replaced by two more general sets.

THEOREM. *There is a monochromatic line for any two nonempty disjoint connected compact sets in* E^2, *whose union is not contained in a straight line.*

To prove this we will use the following lemma:

LEMMA. *Let A and B be nonempty compact connected disjoint subsets of the closed positive quadrant in the x-y plane. Let the origin, p, be in A, $b \in B$ be on the x axis, and $b' \in B$ be on the y axis.*

If $\theta_1 = \sup\{\measuredangle xbp \mid x \in A\}$ *and* $\theta_2 = \sup\{\measuredangle xbp \mid x \in B - \{b\}\}$, *then* $\theta_1 < \theta_2$.

Proof. Note that θ_1 is attained since A is compact. Let $q \in A$ be such that $\theta_1 = \measuredangle qbp$.

Let R denote the unbounded component of $E^2 - B$ and let F be the boundary of R. Then

(1) F is connected [**2**, p. 124],

(2) $F \subset B$ [**3**, p. 635, Paragraph #2],

(3) $b, b' \in F$,

(4) $p, q \in R$,

(5) if y is in the interior of the negative quadrant and $L = (by] \cup (b'y]$, then $L \subseteq R$ and $L \cap A = \phi$.

By [**4**, 3.5 on p. 110] $R - L$ is the union of two components, call one of them C. Notice that the boundary G of C must be contained in $F \cup L$.

Suppose that $\theta_2 \leqq \theta_1$. Then p and q must be in different components of $R - L$, so by [**2**, 1.3 on p. 73] $A \cap G \neq \phi$. But $A \cap L = \phi$, so $A \cap F \neq \phi$. Thus, since $F \subset B$, $A \cap B \neq \phi$. This is a contradiction, so $\theta_1 < \theta_2$.

This lemma easily generalizes to the following: if l and l' are two lines (corresponding to the coordinate axis above) and A and B are two nonempty disjoint connected compact sets such that

(1) $p = l \cap l' \in A$,

(2) there are b, $b' \in B$ with $b \in l$, and $b' \in l'$,

(3) $A \cup B$ is in one of the four closed regions determined by l and l', then with θ_1 and θ_2 defined as above, $\theta_1 < \theta_2$.

Proof of the Theorem. Let a be any point in E^2 and let $r = \sup\{d(a,x) | x \in A \cup B\}$. Since $A \cup B$ is compact, r is attained by some $p \in A \cup B$. Assume $p \in A$.

Let $C = \{x \mid d(a,x) \leqq r\}$ and let m be tangent to C at p. Then $A \cup B$ lies on one side of m. Clearly $A \cap m = \{p\}$ and $B \cap m = \phi$. Let s be a point on m to the "left" of p.

If $x \in A \cup B - \{p\}$, then $0 < \measuredangle spx < \pi$. By the compactness of B, points b, $b' \in B$ exist such that $\measuredangle spb = \inf\{\measuredangle spx \mid x \in B\}$ and $\measuredangle spb' = \sup\{\measuredangle spx \mid x \in B\}$. Clearly $\measuredangle spb \leqq \measuredangle spb'$ and if $x \in B$, then $\measuredangle spb \leqq \measuredangle spx \leqq \measuredangle spb' < \pi$ so $0 \leqq \measuredangle spx - \measuredangle spb = \measuredangle bpx \leqq \measuredangle spb' - \measuredangle spb = \measuredangle bpb' < \pi - \measuredangle spb < \pi$.

Assume there is a point $q \in A$ such that $\measuredangle spq < \measuredangle spb$. If $y \in B \cap pq$, then $\measuredangle spy = \measuredangle spq < \measuredangle spb$ which contradicts the choice of b. Hence $B \cap pq = \phi$, and so pq is a monochromatic line. Similarly, if there exists a point $q \in A$ such that $\measuredangle spq > \measuredangle spb'$, then a monochromatic line exists.

If $\measuredangle bpb' = 0$, then B lies on the line pb, so since $A \cup B$ does not lie on a line, one of the previous cases must occur.

We may now assume:

(1) $0 < \measuredangle bpb' < \pi$ and

(2) if $x \in (A \cup B) - \{p\}$, then $0 \leqq \measuredangle bpx \leqq \measuredangle bpb'$. Note that since we can assume $\measuredangle bpb' > 0$, $b \neq b'$ so $B - \{b\} \neq \phi$.

Let l be the line pb, l' the line pb', $\theta_1 = \sup\{\measuredangle xbp \mid x \in A\}$ and $\theta_2 = \sup\{\measuredangle xbp \mid x \in B - \{b\}\}$. Then A, B, l, and l' are such that the (generalized) lemma applies so $\theta_1 < \theta_2$. Since θ_2 is a supremum there is a $q \in B$ such that $\measuredangle qbp > (\theta_2 - (\theta_2 - \theta_1)) = \theta_1$, hence $qb \cap A = \phi$ and so qb is a monochromatic line.

We now proceed to show that in a certain sense our theorem is the best possible.

(1) Grünbaum [1] considered a finite collection of sets, but in Figures 1 and 2 we find, as did Motzkin, that a monochromatic line does not always exist when we are dealing with more than two sets. In a similar manner we can construct a figure with any finite number of sets which has no monochromatic line.

(2) Figures 3 and 4 show that it is necessary that the sets in our theorem be bounded and closed.

(3) The example shown in Figure 4 depends strongly on the union of the two sets being connected, which cannot happen when both are either open or closed. We will now construct an example of two nonempty open bounded disjoint connected sets which have no monochromatic line.

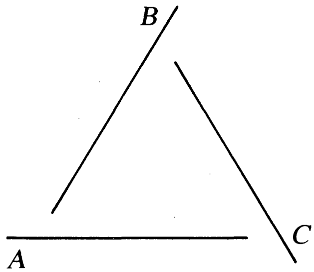


FIG. 1.

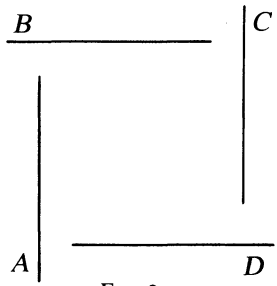


FIG. 2.

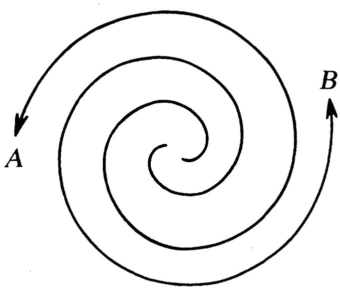


FIG. 3.

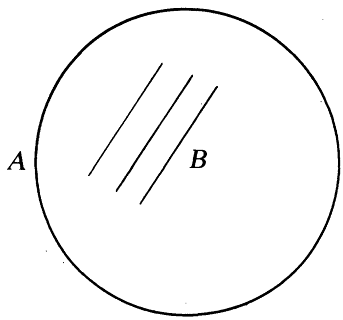


FIG. 4.

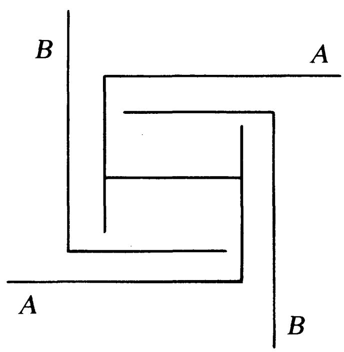


FIG. 5.

Let $S = \{(r, \theta) \mid r = 1 - 1/\theta, 1 \leqq \theta < \infty\}$ and

$$T = \left\{(r, \theta) \mid r = 1 - \frac{1}{\theta + 1}, 1 \leqq \theta < \infty\right\}$$

where (r, θ) are the polar coordinates of a point in the plane. For each $s \in S$ define $p_1(s) = \inf\{(s, t) \mid t \in T\}$, and for each $t \in T$, define $p_2(t) = \inf\{d(t, s) \mid s \in S\}$. Clearly $p_1(s) > 0$ for all $s \in S$ and $p_2(t) > 0$ for all $t \in T$. Let $U = \cup\{B(s, \frac{1}{2}p_1(s)) \mid s \in S\}$ and $V = \cup\{B(t, \frac{1}{2}p_2(t)) \mid t \in T\}$, where $B(y, r) =$

$\{x \mid d(x, y) < r\}$, for any point x and any distance r. Then U and V are easily shown to be disjoint bounded connected open sets. Any line intersecting the region $r < 1$ must intersect both sets, hence no monochromatic line exists.

(4) In [5] the connectedness condition of Grünbaum's theorem was greatly weakened (to assuming the union of the sets was infinite), but Figure 5 shows that connectedness cannot be dispensed with in our theorem.

Set A has only one component, set B has only two, yet there is no monochromatic line.

The preceding examples show that none of the assumptions of our theorem may be omitted; however, they depend heavily on the fact that we are in the plane, so we leave questions open concerning monochromatic lines (and hyperplanes) in higher dimensions.

I wish to thank Dr. M. Edelstein for suggesting the topic and for his guidance and encouragement, and Dr. P. N. Stewart for his help in preparing the manuscript.

References

1. B. Grünbaum, A generalization of a problem of Sylvester, Riveon Lematematika, (1956).

2. M. H. A. Newman, Elements of the Topology of Plane Sets of Points, 2nd ed., University Press, Cambridge, 1951.

3. D. Morrison, M. Kiang and J. Wright, On disjoint connected subsets of a square containing pairs of antipodal points, Canad. Math. Bull., (9) 5 (1966).

4. G. T. Whyburn, Analytic topology, Amer. Math. Soc., Colloq. Publ., 28 (1942), Amer. Math. Soc., New York City.

5. F. Herzog and L. M. Kelly, A generalization of the theorem of Sylvester, Proc. Amer. Math. Soc., 11 (1960).

NOTES ON THE HISTORY OF GEOMETRICAL IDEAS
II. THE PRINCIPLE OF DUALITY

DAN PEDOE, University of Minnesota

In projective geometry we have a remarkable method which produces another, usually distinct theorem, called a *dual* theorem, from any given theorem, by a simple transliteration of the terms involved in the statement of the given theorem. The "dictionary" for the transliteration depends on the space we are working in. We shall restrict ourselves in this note to the plane, in which case, to obtain a dual theorem, we interchange "point" and "line", "lying on" and "passing through", "collinear" and "concurrent", and "intersection" and "join". The Desargues theorem on perspective triangles dualizes to the converse theorem, which can be proved from the direct theorem, so that we say the Desargues theorem is a *self-dual* theorem, and the Pappus theorem dualizes to a theorem which looks different from the given theorem, but can also be proved by the use of the Pappus theorem, so that we say the Pappus theorem is also

$\{x \mid d(x, y) < r\}$, for any point x and any distance r. Then U and V are easily shown to be disjoint bounded connected open sets. Any line intersecting the region $r < 1$ must intersect both sets, hence no monochromatic line exists.

(4) In [5] the connectedness condition of Grünbaum's theorem was greatly weakened (to assuming the union of the sets was infinite), but Figure 5 shows that connectedness cannot be dispensed with in our theorem.

Set A has only one component, set B has only two, yet there is no monochromatic line.

The preceding examples show that none of the assumptions of our theorem may be omitted; however, they depend heavily on the fact that we are in the plane, so we leave questions open concerning monochromatic lines (and hyperplanes) in higher dimensions.

I wish to thank Dr. M. Edelstein for suggesting the topic and for his guidance and encouragement, and Dr. P. N. Stewart for his help in preparing the manuscript.

References

1. B. Grünbaum, A generalization of a problem of Sylvester, Riveon Lematematika, (1956).
2. M. H. A. Newman, Elements of the Topology of Plane Sets of Points, 2nd ed., University Press, Cambridge, 1951.
3. D. Morrison, M. Kiang and J. Wright, On disjoint connected subsets of a square containing pairs of antipodal points, Canad. Math. Bull., (9) 5 (1966).
4. G. T. Whyburn, Analytic topology, Amer. Math. Soc., Colloq. Publ., 28 (1942), Amer. Math. Soc., New York City.
5. F. Herzog and L. M. Kelly, A generalization of the theorem of Sylvester, Proc. Amer. Math. Soc., 11 (1960).

NOTES ON THE HISTORY OF GEOMETRICAL IDEAS
II. THE PRINCIPLE OF DUALITY

DAN PEDOE, University of Minnesota

In projective geometry we have a remarkable method which produces another, usually distinct theorem, called a *dual* theorem, from any given theorem, by a simple transliteration of the terms involved in the statement of the given theorem. The "dictionary" for the transliteration depends on the space we are working in. We shall restrict ourselves in this note to the plane, in which case, to obtain a dual theorem, we interchange "point" and "line", "lying on" and "passing through", "collinear" and "concurrent", and "intersection" and "join". The Desargues theorem on perspective triangles dualizes to the converse theorem, which can be proved from the direct theorem, so that we say the Desargues theorem is a *self-dual* theorem, and the Pappus theorem dualizes to a theorem which looks different from the given theorem, but can also be proved by the use of the Pappus theorem, so that we say the Pappus theorem is also self-dual. These facts are of fundamental importance in the foundations of geometry, and enable us to assert that the so-called Principle of Duality is, in fact, a Theorem of Duality. Karl Menger (pp. 201, 211, [**3**]) writes both fundamental theorems in self-dual forms, so that the transliteration given above does not essentially change the statement of the theorem.

The richness of the applications of duality is enormously increased by the fact that the dual of a conic, considered as a set of points, is a conic considered as a set of tangents (see Section 78.1 in [**4**]). Thus the Pascal and Brianchon theorems are dual theorems for a conic.

The statements in the first paragraph above make no mention of coordinates. If we use homogeneous coordinates (x, y, z) for points in a projective plane, the equation of a line is $uX + vY + wZ = 0$, and we can introduce the homogeneous coordinates $[u, v, w]$ of a line. The condition that the point (x, y, z) should be incident with the line $[u, v, w]$ is

$$ux + vy + wz = 0,$$

and the symmetry of this relation between point-coordinates (x, y, z) and line- (or *tangential*)-coordinates $[u, v, w]$ is the basis for the Theorem of Duality, since in any relation involving points, lines and incidences we can replace (x, y, z) by $[x, y, z]$, and $[u, v, w]$ by (u, v, w), and the incidence relations are undisturbed.

We note that the line $[x, y, z]$ is the polar line of the point (x, y, z) with respect to the conic

$$X^2 + Y^2 + Z^2 = 0 \tag{1}$$

and so the Theorem of Duality can be interpreted as a *Theorem of Reciprocal Polars.* We also note that any polarity of a plane involves a conic as the locus of points which lie on their corresponding polars. For the polar p of a point P is given by the equation $p = \mathbf{A}P$, where $\mathbf{A}$ is a symmetric matrix, and P lies on p if and only if $P^T \mathbf{A} P = 0$. The conic, as in (1), may not contain real points but this in no way invalidates its use as a *deus ex machina.* It is interesting to find that George Salmon (p. 126 of [**8**]) says: "The principle of duality may be established independently of the method of reciprocal polars by showing... that all the equations we employ admit of a two-fold interpretation." Salmon then introduces tangential coordinates for planes (he is working in three dimensions) as we introduced them for lines above. But this is making unconscious use of the god in the machine, the quadric surface

$$X^2 + Y^2 + Z^2 + T^2 = 0. \tag{2}$$

Veblen and Young (p. 29, [**9**]) say: "The Principle of Duality was first stated explicitly by Gergonne (1826), but was led up to by the writings of Poncelet and others during the first quarter of the 19th century." Controversy as to priority clouded a large part of Poncelet's life. In a supplement to the second edition (1866) of the second volume of his great *Traité des Propriétés Projectives des*

Figures [7], first published in 1822, Poncelet devotes 132 large pages in small print to diatribes against the many geometers who seemed not to be on his side in this controversy. He attacks Gergonne, of course, but also Plücker and Möbius, each of whom claimed independent discovery of the Principle of Reciprocal Polars; but Poncelet reserves very special blasts for Chasles, remarking acidly that Cremona had called Chasles *the Archimedes*, and that de Jonquières had named him *the La Fontaine* of modern geometry! Poncelet also has sideswipes at Cayley, remarks with surprise that Sylvester writes good French, and even brings in Salmon, referring to the professor of divinity as *un journaliste philosophe*, with a reference to a footnote on p. 241 of the 1862 edition of Salmon's *Analytical Geometry of Three Dimensions*, which I have not been able to locate.

Amidst all this smoke there is little fire. However, Poncelet does accuse Gergonne (p. 375, II, [7]) of stating that the number of tangents or tangent planes common to two curves or three surfaces is equal to the product of the degrees of their equations, which is certainly incorrect. In fact, Poncelet asserts that the Principle of Duality, as enunciated and used by Gergonne and his supporters, cannot deal with metrical theorems either. It should be stated at this point that the method of reciprocal polars, called *point reciprocation*, when applied to circles, using a circle as fundamental conic, produces theorems about conics and their foci or, conversely, produces theorems about circles from given theorems about conics and their foci ([**2**]: see also [**5**]). The Principle of Duality can hardly transform theorems in this way.

Positive statements about the Poncelet-Gergonne rivalry are rare, but before we discuss one made by Coxeter, an acid comment made by Plücker is worth noting (F. N. VI, vol. II [**6**]). Plücker is commenting on the alleged superiority of the Gergonne Principle of Duality:

"Above all, every thought which does not immediately arise from the nature of the case, but is taken over from a metaphysical abstraction, easily exercises a dictatorial rule over us, which always carries its own punishment, imposing bonds on unrestricted modes of thought." (*Jeder Gedanke überhaupt, der nicht aus der Natur der Sache unmittelbar entspringt, sondern aus einer metaphysischen Abstraction übertragen wird, übt so leicht eine dictatorische Herrschaft über uns aus und führt dann seine Strafe immer mit sich, indem er dem unbefangenen Gedankengange Fesseln anlegt.*)

Coxeter, in an exercise (2, p. 75, [**1**]), asserts that Gergonne must be regarded as the victor in his historic contest with Poncelet. Coxeter first shows that the Desargues configuration is self-polar (p. 74), points in the configuration mapping onto lines in the configuration in a certain polarity, and then considers the Pappus configuration. It turns out that this is self-polar if and only if three lines in the configuration are concurrent, which would involve a specialization of the Pappus configuration. Coxeter then says: "Since the general Pappus configuration is self-dual without being self-polar, the old controversy between Poncelet and Gergonne is settled in the latter's favour."

I feel that this is a judgement against which history must appeal, that the criteria used are not valid, and seem to depend, in the final analysis, on a semantic misunderstanding. If we call the Principle of Reciprocal Polars (P), and the Principle of Duality (G), then application of (P) to any theorem in the projective plane, using the fundamental conic (1), the ground field being that of the complex numbers, produces a theorem identical with that obtained by applying (G), and no more specialized, as far as the figure goes, than that obtained by applying (G). For any specialization of the dual figure, obtained by applying (P), which involves the lines p_i and the points P_j, implies a specialization of the initial figure involving the *points* p_i and the *lines* P_j.

On the other hand, the application of (P) produces theorems which cannot be produced by (G), as we have already remarked. It is possible that (G) may operate outside the regions of projective geometry over the complex numbers, as a general property of the space (*une propriété générale de l'étendue*), to quote the Gergonne phrase which disturbed Plücker, where (P) may have no validity, there being no conics, for instance, and further discussions on this ancient but fascinating controversy are surely to be welcomed.

References

1. H. S. M. Coxeter, The Real Projective Plane, Cambridge University Press, Cambridge, 1955.

2. C. V. Durell, Projective Geometry, Macmillan, London, 1945.

3. K. Menger (and L. M. Blumenthal), Studies in Geometry, Freeman, San Francisco, 1970.

4. D. Pedoe, A Course of Geometry for Colleges and Universities, Cambridge University Press, New York, 1970.

5. ———, The most elementary theorem of Euclidean geometry, this MAGAZINE, to appear.

6. J. Plücker, Analytisch-Geometrische Entwicklungen, Baedeker, Essen, vol. I, 1828, vol. II, 1831.

7. J. V. Poncelet, Traité des Propriétés Projectives des Figures, 2nd. ed., Paris, vol. I, 1865, vol. II, 1866.

8. G. Salmon, A Treatise on the Analytical Geometry of Three Dimensions, Longmans, London, 1928.

9. O. Veblen and J. W. Young, Projective Geometry, Ginn, New York, vol. I, 1938, vol. II, 1946.

A NOTE ON CONSECUTIVE COMPOSITE INTEGERS

E. F. ECKLUND, JR., Northern Illinois University, and
R. B. EGGLETON, The University of Calgary

1. Introduction. In this note we give a new and elementary proof of the following result: *Among any four consecutive integers greater than* 11, *there is always at least one divisible by a prime greater than* 11.

This result belongs to the theory of the number-theoretic function f, defined for each positive integer k so that $f(k)$ is the smallest positive integer with the property that among any $f(k)$ consecutive integers greater than k there is always

I feel that this is a judgement against which history must appeal, that the criteria used are not valid, and seem to depend, in the final analysis, on a semantic misunderstanding. If we call the Principle of Reciprocal Polars (P), and the Principle of Duality (G), then application of (P) to any theorem in the projective plane, using the fundamental conic (1), the ground field being that of the complex numbers, produces a theorem identical with that obtained by applying (G), and no more specialized, as far as the figure goes, than that obtained by applying (G). For any specialization of the dual figure, obtained by applying (P), which involves the lines p_i and the points P_j, implies a specialization of the initial figure involving the *points* p_i and the *lines* P_j.

On the other hand, the application of (P) produces theorems which cannot be produced by (G), as we have already remarked. It is possible that (G) may operate outside the regions of projective geometry over the complex numbers, as a general property of the space (*une propriété générale de l'étendue*), to quote the Gergonne phrase which disturbed Plücker, where (P) may have no validity, there being no conics, for instance, and further discussions on this ancient but fascinating controversy are surely to be welcomed.

References

1. H. S. M. Coxeter, The Real Projective Plane, Cambridge University Press, Cambridge, 1955.

2. C. V. Durell, Projective Geometry, Macmillan, London, 1945.

3. K. Menger (and L. M. Blumenthal), Studies in Geometry, Freeman, San Francisco, 1970.

4. D. Pedoe, A Course of Geometry for Colleges and Universities, Cambridge University Press, New York, 1970.

5. ———, The most elementary theorem of Euclidean geometry, this MAGAZINE, to appear.

6. J. Plücker, Analytisch-Geometrische Entwicklungen, Baedeker, Essen, vol. I, 1828, vol. II, 1831.

7. J. V. Poncelet, Traité des Propriétés Projectives des Figures, 2nd. ed., Paris, vol. I, 1865, vol. II, 1866.

8. G. Salmon, A Treatise on the Analytical Geometry of Three Dimensions, Longmans, London, 1928.

9. O. Veblen and J. W. Young, Projective Geometry, Ginn, New York, vol. I, 1938, vol. II, 1946.

A NOTE ON CONSECUTIVE COMPOSITE INTEGERS

E. F. ECKLUND, JR., Northern Illinois University, and
R. B. EGGLETON, The University of Calgary

1. Introduction. In this note we give a new and elementary proof of the following result: *Among any four consecutive integers greater than* 11, *there is always at least one divisible by a prime greater than* 11.

This result belongs to the theory of the number-theoretic function f, defined for each positive integer k so that $f(k)$ is the smallest positive integer with the property that among any $f(k)$ consecutive integers greater than k there is always at least one divisible by a prime greater than k. (Equivalently, the longest run of consecutive composite integers greater than k with no prime factor exceeding k contains $f(k)-1$ members.) A survey of known results concerning f is given in [**1**]. The result under study in this note is $f(11)=4$; our proof, which needs no recourse to computer calculation, is in the spirit of Utz's paper [**5**].

2. Plan of attack. The essential idea of the proof, given in section 5, is to obtain a contradiction from the fact that if there were four consecutive integers greater than 11 with no prime factor exceeding 11, the distribution of the few available prime factors among the four integers would require the existence of a related solution to one or other of a set of Diophantine equations. These equations are solved in section 4, basically by establishing an upper bound on solutions. The main tool in obtaining this upper bound is the lemma in section 3. This is essentially a result of Sylvester [**4**], extended to include precise information in the exceptional as well as the regular case. In fact, the regular part of the lemma can be deduced readily from Theorems 4–5 and 4–6 of [**3**], for example. However, we prefer to give a proof which is self-contained, and direct rather than inductive.

3. The power of p in a^n-1. With p any fixed prime, let α be the number-theoretic function defined by $p^{\alpha(k)}\| k!$ for each positive integer k. (The notation $p^\alpha \| n$ indicates that the power of p in n is α, that is, $p^\alpha \mid n$ but $p^{\alpha+1}\nmid n$.) If p^m is the largest power of p not exceeding k, note that

$$(1)\qquad \alpha(k)=\sum_{r=1}^{m}[k/p^r]\leqq \sum_{r=1}^{m} k/p^r = k(1-1/p^m)/(p-1)\leqq (k-1)/(p-1),$$

where the case $m=0$ is included by the convention that empty sums have value zero. We use (1) in proving the following result:

LEMMA (Sylvester). *For any prime p and positive integer n, let $a\neq 1$ be an integer (not necessarily positive) such that $p^\lambda \| a-1$ and $p^\mu \| n$, where $\lambda \geqq 1$, $\mu\geqq 0$. Then $p^{\lambda+\mu}\| a^n-1$ except when $p=2$, $\lambda=1$, $\mu\geqq 1$. In the exceptional case let $n=2^\mu\nu$ and $2^\kappa \| a^\nu+1$; then $2^{\kappa+\mu}\| a^n-1$.*

Proof. (i) Let $b=a-1$, so $a^n-1=\Sigma_{k=1}^{n}\binom{n}{k}b^k$. The first term of this series is bn, and $p^{\lambda+\mu}\| bn$. If each subsequent term is divisible by a higher power of p, the result $p^{\lambda+\mu}\| a^n-1$ certainly follows. Now

$$(2)\qquad \binom{n}{k}b^k=\frac{b^{k-1}}{k!}\cdot bn\cdot\frac{(n-1)!}{(n-k)!}\quad\text{for}\quad 1\leqq k\leqq n,$$

and the third factor on the right is an integer, so if the power of p in $k!$ is less than that in b^{k-1} when $2\leqq k\leqq n$, then the power of p in $\binom{n}{k}b^k$ exceeds that in bn. Thus we want $\alpha(k)<(k-1)\lambda$, which is ensured by (1) if $p\geqq 3$ or $\lambda\geqq 2$. Hence $p^{\lambda+\mu}\| a^n-1$ if $p\geqq 3$ or $\lambda\geqq 2$.

(ii) Now take $p = 2$, $\lambda = 1$, $\mu = 0$. Then $2^1 \| bn$ and $2^2 \Big| \binom{n}{k} b^k$ if $2 \leqq k \leqq n$, since the third factor on the right of (2) contains the even factor $n-1$ if $2 \leqq k \leqq n$. Hence $2^1 \| a^n - 1$, conforming to the regular case.

(iii) Finally take $p = 2$, $\lambda = 1$, $\mu \geqq 1$. With $n = 2^\mu \nu$, let $c = a^\nu$ and $2^\kappa \| c + 1$. Since $2^1 \| a - 1$ and ν is odd. $c \equiv -1 \pmod 4$ and $c^{2^r} \equiv 1 \pmod 4$ for $r \geqq 1$. Thus $2^1 \| c - 1$ and $2^1 \| c^{2^r} + 1$ for $r \geqq 1$, so $2^{\kappa+\mu} \| a^n - 1$ is implied by

$$a^n - 1 = c^{2^\mu} - 1 = (c-1) \prod_{r=0}^{\mu-1} (c^{2^r} + 1). \quad ∎$$

4. Solutions to the relevant Diophantine equations. Let $[p, q, k]$ denote the exponential Diophantine equation $|p^x - kq^y| = 1$, where p, q are given primes, k is a given positive integer and x, y are positive integers to be determined. We shall now use the lemma to obtain complete solutions for a set of equations of this form. We specify the solutions in the implicit form (p^x, kq^y) rather than the explicit form (x, y).

A. *Solutions of* [2, 3, 1] *and other equations with* $k = 1$. To solve [2, 3, 1], let $2^\mu \| y$. The lemma shows $2^{\mu+2} \| (1-2^2)^y - 1$, so $2^1 \| (1-2^2)^y + 1$. Thus if $\mu = 0$, $2^2 \| 3^y + 1$ and $2^1 \| 3^y - 1$. Then $2^x = 3^y + 1 \Rightarrow x = 2$, yielding the solution (4, 3); $2^x = 3^y - 1 \Rightarrow x = 1$, yielding (2, 3). If $\mu \geqq 1$, $2^{\mu+2} \| 3^y - 1$ and $2^1 \| 3^y + 1$. Then $2^x = 3^y + 1 \Rightarrow x = 1$, contradicting $y > 0$. Also $2^x = 3^y - 1 \Rightarrow x = \mu + 2$, so $2^\mu \| y$ leads to the bound $y \geqq 2^\mu = 2^{x-2} = (3^y - 1)/4$, satisfied only if $y \leqq 2$; hence $\mu \geqq 1$ yields the solution (8, 9). ∎

The four equations we shall need which are amenable to this form of argument are as follows:

	Equation	*Solutions*	*Argument uses*
1.	[2, 3, 1]	(2, 3) (4, 3) (8, 9)	$2^{\mu+2} \| (1-2^2)^y - 1.$
2.	[2, 5, 1]	(4, 5)	$2^{\mu+2} \| (1+2^2)^y - 1.$
3.	[2, 7, 1]	(8, 7)	$2^{\mu+3} \| (1-2^3)^y - 1.$
4.	[2, 11, 1]	none	$2^{\mu+2} \| (1-2^2 \cdot 3)^y - 1.$

B. *Solutions of* [3, 5, 2] *and other equations with* $k = 2$. To solve [3, 5, 2], put $x = 4z + r$, where $0 \leqq r \leqq 3$. Then $3^x - 2 \cdot 5^y = \pm 1 \Rightarrow 3^r \equiv \pm 1 \pmod 5 \Rightarrow r = 0, 2$ respectively. Thus $3^x - 2 \cdot 5^y = 1 \Rightarrow 2 \cdot 5^y = (2 \cdot 5 - 1)^{2z} - 1$, but by the lemma $2^2 | (1 - 2 \cdot 5)^{2z} - 1$ so $2^2 | 2 \cdot 5^y$, a contradiction. Also $3^x - 2 \cdot 5^y = -1 \Rightarrow 2 \cdot 5^y = (2 \cdot 5 - 1)^{2z+1} + 1$, so if $5^\mu \| 2z + 1$ the lemma ensures $5^{\mu+1} \| (1 - 2 \cdot 5)^{2z+1} - 1 \Rightarrow 5^{\mu+1} \| 2 \cdot 5^y \Rightarrow y = \mu + 1$. But $x = 4z + 2$ so $5^\mu \| 2z + 1$ leads to the bound $x \geqq 2 \cdot 5^\mu = 2 \cdot 5^{y-1} = (3^x + 1)/5$, satisfied only if $x \leqq 2$. This yields the solution (9, 10). ∎

The twelve equations we shall need which are amenable to this form of argument are as follows:

	Equation	*Solutions*	*Argument uses*
1.	[3, 5, 2]	(9, 10)	$x = 4z + r$.
2.	[3, 7, 2]	none	$x = 6z + r$.
3.	[3, 11, 2]	(243, 242)	$x = 5z + r$.
4.	[5, 3, 2]	(5, 6)	$x = 2z + r$.
5.	[5, 7, 2]	none	$x = 6z + r$.
6.	[5, 11, 2]	none	$x = 5z + r$.
7.	[7, 3, 2]	(7, 6)	x unmodified.
8.	[7, 5, 2]	(49, 50)	$x = 4z + r$.
9.	[7, 11, 2]	none	$x = 10z + r$.
10.	[11, 3, 2]	none	$x = 2z + r$.
11.	[11, 5, 2]	(11, 10]	x unmodified.
12.	[11, 7, 2]	none	$x = 3z + r$.

With further theoretical development, a more systematic and comprehensive method of solving equations of the form $[p, q, k]$ can be given. This is indicated in a forthcoming paper [**2**].

5. Main proof. The results in section 4 can now be applied to establish the desired result:

THEOREM. $f(11) = 4$.

Proof. The sequence 14, 15, 16 shows $f(11) \geqq 4$. Equality follows by contradiction from the supposition that there is a sequence S of four consecutive integers greater than 11, none of which has a prime factor exceeding 11.

Suppose two terms of S have no prime factor exceeding 3. They have difference δ, where $1 \leqq \delta \leqq 3$, so both can be divided by δ to give a power of 2 and a power of 3 with difference 1, corresponding to a solution of [2, 3, 1]. With $\delta = 1$, there are no such pairs exceeding 11; with $\delta = 2$, the only possible pair is 16, 18 but $17 \in S$ is precluded; with $\delta = 3$, the only possible pair is 24, 27 but $26 = 2 \cdot 13 \in S$ is precluded. Hence S can only have 5, 7, 11 occurring as factors of three different members with the fourth having no prime factor exceeding 3.

Let the consecutive members of S be a, b, c, d without specifying whether the order is increasing or decreasing, so there is no loss of generality in assuming that the term with no prime factor exceeding 3 is either a or b. If it is a, there are six possibilities. (Here p, q denote distinct primes chosen from among 5, 7, 11.)

1. $2^2 \cdot 3 \mid a \Rightarrow b = p^x,\ c = 2q^y \Rightarrow (b, c)$ satisfies $[p, q, 2]$.
2. $a = 2 \cdot 3^y \Rightarrow b = p^x \Rightarrow (b, a)$ satisfies $[p, 3, 2]$.
3. $a = 2^x,\ 3 \nmid b \Rightarrow b = q^y \Rightarrow (a, b)$ satisfies $[2, q, 1]$.
4. $a = 2^x,\ 3 \mid b \Rightarrow c = 2q^y \Rightarrow (a/2, c/2)$ satisfies $[2, q, 1]$.
5. $a = 3^x,\ 2^1 \| b \Rightarrow b = 2q^y \Rightarrow (a, b)$ satisfies $[3, q, 2]$.
6. $a = 3^x,\ 2^2 \mid b \Rightarrow d = 6q^y \Rightarrow (a/3, d/3)$ satisfies $[3, q, 2]$.

If b is the term with no prime factor exceeding 3, there are also six possibilities.

7. $2^2 \cdot 3 | b \Rightarrow c = p^x$, $d = 2q^y \Rightarrow (c, d)$ satisfies $[p, q, 2]$.
8. $b = 2 \cdot 3^y \Rightarrow a = p^x \Rightarrow (a, b)$ satisfies $[p, 3, 2]$.
9. $b = 2^x$, $3 \nmid a \Rightarrow a = q^y \Rightarrow (b, a)$ satisfies $[2, q, 1]$.
10. $b = 2^x$, $3 | a \Rightarrow c = q^y \Rightarrow (b, c)$ satisfies $[2, q, 1]$.
11. $b = 3^x$, $2^1 \| a \Rightarrow a = 2q^y \Rightarrow (b\,a)$ satisfies $[3, q, 2]$.
12. $b = 3^x$, $2^2 | a \Rightarrow c = 2q^y \Rightarrow (b, c)$ satisfies $[3, q, 2]$.

By section 4, every possibility requires S to include a term with a prime factor exceeding 11, which is forbidden. Thus S does not exist. ∎

The authors are indebted to Professor R. K. Guy for several expository improvements.

References

1. E. F. Ecklund, Jr., and R. B. Eggleton, Prime factors of consecutive integers, Amer. Math. Monthly, 79 (1972) 1082–1089.
2. R. B. Eggleton and J. L. Selfridge, Factors of neighbours to a perfect power, to appear.
3. W. J. LeVeque, Topics in Number Theory, vol. I, Addison-Wesley, Reading, 1956.
4. J. J. Sylvester, Sur une classe spéciale des diviseurs de la somme d'une série géometrique, C. R. Acad. Sci. Paris, 107 (1888) 446–450; Collected Mathematical Papers, vol. 4, 1912, p. 607, *et seq.*
5. W. R. Utz, A conjecture of Erdös concerning consecutive integers, Amer. Math. Monthly, 68 (1961) 896–897.

AN EXTREMAL PROBLEM OF GRAPHS WITH DIAMETER 2

BÉLA BOLLOBÁS and PAUL ERDÖS, University of Cambridge, England

Let $1 \leqq k < p$. We say that a graph has property $P(p, k)$ if it has p points and every two of its points are joined by at least k paths of length $\leqq 2$. The aim of this note is to discuss the following problem. At least how many edges are in a graph with property $P(p, k)$? Denote this minimum by $m(p, k)$.

Construct a graph $G_0(p, k)$ with property $P(p, k)$ as follows. Take two classes of points, k in the first class and $p - k$ in the second, and take all the edges incident with at least one point in the first class. Thus $G_0(p, k)$ has $\binom{p}{2} - \binom{p-k}{2}$ edges.

Murty [2] proved that if $p \geqq \frac{1}{2}(3 + \sqrt{5})k$ then $m(p, k) = \binom{p}{2} - \binom{p-k}{2}$ and $G_0(p, k)$ is the only graph with property $P(p, k)$ that has $m(p, k)$ edges. He also suspected that the same result holds already for $p > 2k$. We shall show that this is not so, in fact $p \geqq \frac{1}{2}(3 + \sqrt{5})k$ is almost necessary for $G_0(p, k)$ to be an extremal graph, and we determine the asymptotic value of $m([ck], k)$ for every constant $1 < c < \frac{1}{2}(3 + \sqrt{5})$, where $[x]$ denotes the integer part of x.

If b is the term with no prime factor exceeding 3, there are also six possibilities.

7. $2^2 \cdot 3 | b \Rightarrow c = p^x$, $d = 2q^y \Rightarrow (c, d)$ satisfies $[p, q, 2]$.
8. $b = 2 \cdot 3^y \Rightarrow a = p^x \Rightarrow (a, b)$ satisfies $[p, 3, 2]$.
9. $b = 2^x$, $3 \nmid a \Rightarrow a = q^y \Rightarrow (b, a)$ satisfies $[2, q, 1]$.
10. $b = 2^x$, $3 | a \Rightarrow c = q^y \Rightarrow (b, c)$ satisfies $[2, q, 1]$.
11. $b = 3^x$, $2^1 \| a \Rightarrow a = 2q^y \Rightarrow (b a)$ satisfies $[3, q, 2]$.
12. $b = 3^x$, $2^2 | a \Rightarrow c = 2q^y \Rightarrow (b, c)$ satisfies $[3, q, 2]$.

By section 4, every possibility requires S to include a term with a prime factor exceeding 11, which is forbidden. Thus S does not exist. ∎

The authors are indebted to Professor R. K. Guy for several expository improvements.

References

1. E. F. Ecklund, Jr., and R. B. Eggleton, Prime factors of consecutive integers, Amer. Math. Monthly, 79 (1972) 1082–1089.

2. R. B. Eggleton and J. L. Selfridge, Factors of neighbours to a perfect power, to appear.

3. W. J. LeVeque, Topics in Number Theory, vol. I, Addison-Wesley, Reading, 1956.

4. J. J. Sylvester, Sur une classe spéciale des diviseurs de la somme d'une série géometrique, C. R. Acad. Sci. Paris, 107 (1888) 446–450; Collected Mathematical Papers, vol. 4, 1912, p. 607, *et seq.*

5. W. R. Utz, A conjecture of Erdös concerning consecutive integers, Amer. Math. Monthly, 68 (1961) 896–897.

AN EXTREMAL PROBLEM OF GRAPHS WITH DIAMETER 2

BÉLA BOLLOBÁS and PAUL ERDÖS, University of Cambridge, England

Let $1 \leqq k < p$. We say that a graph has property $P(p, k)$ if it has p points and every two of its points are joined by at least k paths of length $\leqq 2$. The aim of this note is to discuss the following problem. At least how many edges are in a graph with property $P(p, k)$? Denote this minimum by $m(p, k)$.

Construct a graph $G_0(p, k)$ with property $P(p, k)$ as follows. Take two classes of points, k in the first class and $p - k$ in the second, and take all the edges incident with at least one point in the first class. Thus $G_0(p, k)$ has $\binom{p}{2} - \binom{p-k}{2}$ edges.

Murty [2] proved that if $p \geqq \frac{1}{2}(3 + \sqrt{5})k$ then $m(p, k) = \binom{p}{2} - \binom{p-k}{2}$ and $G_0(p, k)$ is the only graph with property $P(p, k)$ that has $m(p, k)$ edges. He also suspected that the same result holds already for $p > 2k$. We shall show that this is not so, in fact $p \geqq \frac{1}{2}(3 + \sqrt{5})k$ is almost necessary for $G_0(p, k)$ to be an extremal graph, and we determine the asymptotic value of $m([ck], k)$ for every constant $1 < c < \frac{1}{2}(3 + \sqrt{5})$, where $[x]$ denotes the integer part of x.

THEOREM. *Let* $1 < c < \frac{1}{2}(3+\sqrt{5})$, $p = [ck]$. *Then* $m(p,k) = c^{3/2}k^2/2 + o(k^2)$.

Proof. Exactly as in [2] (or by a simple counting argument) one can show that

$$m(p,k) \geqq c^{3/2}k^2/2 + O(k).$$

Therefore the problem is to prove an upper bound for $m(p,k)$, i.e., to construct graphs with property $P(p,k)$ that have few edges.

Let $\varepsilon > 0$. Take $p = [ck]$ points and choose each edge with probability $d = c^{-\frac{1}{2}} + \varepsilon$. The law of large numbers implies that, as $k \to \infty$, with probability tending to 1, this graph $G_1(p,k)$ has $\binom{p}{2}(d + o(1))$ edges. Also, by another simple application of the law of large numbers, we obtain that with probability tending to 1 for every two of the points there are $(d^2 + o(1))p$ points joined to both of them. Thus as $p \to \infty$ with probability tending to 1 this graph $G_1(p,k)$ has property $P(p,k)$ and it has $\leqq (d^2+\varepsilon)\binom{p}{2}$ edges, proving the required inequality.

If the reader is not familiar with the probabilistic terminology or does not like it, we suggest the following combinatorial translation.

Consider all graphs on a set V of p labelled points having $\binom{p}{2}d = q$ edges. The number of these graphs is $\binom{Q}{q}$, where $Q = \binom{p}{2}$. Let a, b be two arbitrary points and let $x < k$ be an integer. Let us compute the number of graphs in which there are exactly x points joined to both a and b. If there are x points joined to both a and b, there are y points in $V - \{a,b\}$ joined to a and there are z points in $V - \{a,b\}$ joined to b; then the edges incident with exactly one of the points a, b can be chosen in

$$\binom{p-2}{x}\binom{p-2-x}{y}\binom{p-2-x-y}{z}$$

different ways. The remaining edges of the graph can be chosen in $\binom{Q'}{q-e}$ ways, where $Q' = \binom{p-2}{2} + 1$ and $e = 2x + y + z$. Consequently the number of graphs in question is

$$\sum_{x+y+z \leqq p-2} \binom{p-2}{x}\binom{p-2-x}{y}\binom{p-2-x-y}{z}\binom{Q'}{q-e},$$

where the summation goes over all pairs of nonnegative integers (y,z) satisfying $x + y + z \leqq p - 2$. Thus there are at most

$$\binom{n}{2}\sum_{x+y+z \leqq p-2} \binom{p-2}{x}\binom{p-2-x}{y}\binom{p-2-x-y}{z}\binom{Q'}{q-e}$$

graphs not having property $P(p,k)$. By a simple but laborious estimation one can prove that if k is sufficiently large then this is less than $\binom{Q}{q}$ (in fact the sum divided by $\binom{Q}{q}$ tends to zero as $k \to \infty$). This proves that if k is sufficiently large there exists a graph with q edges that has property $P(p, k)$.

REMARKS. 1. With a slight improvement of the same method one can prove that if

$$[ck] = p < \frac{3+\sqrt{5}}{2} k - k^{\frac{1}{2}}(\log k)^{\alpha}$$

(α sufficiently large) then $m(p, k) = c^{3/2}k^2/2 + o(k^2)$ and *the graph* $G_0(p, k)$ *is not extremal.*

A problem similar to the one discussed here and in [2] was solved in [1]. By the method applied there one could improve the result in [2] slightly. One could show that $G_0(p, k)$ is extremal in a larger range than $p \geqq \frac{1}{2}(3+\sqrt{5})k$, but the method would not bring the lower bound on p down to $\frac{1}{2}(3+\sqrt{5})k - k^{\frac{1}{2}}(\log k)^{\alpha}$.

It would be of interest to determine as accurately as possible the smallest value $p = p(k)$ for which the graph $G_0(p, k)$ is extremal. Furthermore in the range where $G_0(p, k)$ is not extremal determine (again as accurately as possible) $m(p, k)$ and characterize the extremal graphs.

2. One can also give a nonprobabilistic proof of the theorem. As before, let

$$1 < c < \tfrac{1}{2}(3+\sqrt{5}), \qquad \varepsilon > 0, \qquad d = c^{-\frac{1}{2}} + \varepsilon.$$

Furthermore, let p be a natural number and $\alpha = \alpha(p)$ a real number. Denote by $G_1(p, \alpha, d)$ the following graph. The points are $\{1, 2, \cdots, p\}$, and i is joined to j if

$$(i-j)^2\alpha - [(i-j)^2\alpha] < d.$$

It suffices to show that $\alpha = \alpha(p)$ can be chosen in a such a way that if p is sufficiently large $G_1(p, \alpha, d)$ has property $P(p, k)$ and has $\frac{1}{2}dn^2 + o(n^2)$ edges. It indeed follows from well-known theorems on diophantine approximation that $G_1(p, \alpha, d)$ has $\frac{1}{2}dp^2 + o(p^2)$ edges, provided α is irrational. The graph has property $P(p, k)$ if whenever $1 \leqq i < j \leqq p$, the number of integers t, $1 \leqq t \leqq p$, for which

$$(t-i)^2\alpha - [(t-i)^2\alpha] < d \quad \text{and} \quad (t-j)^2\alpha - [(t-j)^2\alpha] < d,$$

is $d^2p + o(p)$ uniformly in i and j. (For sufficiently large p clearly $d^2p + o(p) > k$.) We could not prove this but Cassels showed that this holds if we choose $\alpha = \alpha(p) = 1/q$, where q is the smallest prime not less than p. The proof uses analytic number theory and will not be given here. The same choice of α also ensures that G_1 has $\frac{1}{2}dp^2 + o(p^2)$ edges. This result completes the proof of the theorem.

It would still be of interest to prove the result for every irrational α.

References

1. B. Bollobás and S. Eldridge, On graphs with diameter 2, to appear in J. Combinatorial Theory.

2. U. S. R. Murty, On critical graphs of diameter 2, this MAGAZINE, 41 (1968) 138–140.

WHEN IS -1 A POWER OF 2?

MAN KEUNG SIU, University of Hong Kong

A more precise statement of the question posed in the title is the following: *When is the equation*

$$(\#) \qquad 2^x + 1 \equiv 0 \pmod{d}$$

solvable? It is obvious that the answer is in the negative when d is even. Henceforth d is assumed to be a positive *odd* integer greater than 1.

Translating into group-theoretic language, we are asking: *When does the subgroup* $\langle 2 \rangle$ *in* $(Z/dZ)^*$ *contain* -1? Here $(Z/dZ)^*$ denotes the multiplicative group of all units in Z/dZ and $\langle 2 \rangle$ denotes the cyclic subgroup generated by 2. We shall denote the order of $\langle 2 \rangle$ by r. In other words, r is the smallest positive integer such that $2^r \equiv 1 \pmod{d}$.

An immediate (but seemingly somewhat useless) criterion for the solvability of $(\#)$ is as follows:

LEMMA 1. $(\#)$ *is solvable if and only if r is even and* $2^{r/2} + 1 \equiv 0 \pmod{d}$.

Proof. The sufficiency is trivial. For the necessity, assume $(\#)$ has a solution. Then it certainly has one with $x < r$. (You need d odd to do this.) Then $1 = (-1)^2 \equiv 2^{2x} \pmod{d}$, so r divides $2x$. That is, $2x = rk$ for some integer k. But $x < r$, so $k = 1$ and $x = r/2$. Q.E.D.

We can improve Lemma 1 a little bit if d is a power of an odd prime.

LEMMA 2. *If d is a power of an odd prime, then $(\#)$ is solvable if and only if r is even.*

Proof. The necessity has been shown in Lemma 1. For the sufficiency, first observe that $\langle 2 \rangle$ is a subgroup of the *even order cyclic* group $(Z/dZ)^*$ (if $d = p^k$, then $(Z/dZ)^*$ is in fact the direct product of the cyclic groups $Z/p^{k-1}Z$ and $Z/(p-1)Z$), and $\langle 2 \rangle$ contains an element of order two (namely, the element $2^{r/2}$). It remains to show -1 is the *unique* element of order two in $(Z/dZ)^*$, for then it follows $-1 \in \langle 2 \rangle$. More generally, we shall show a cyclic group of even order contains exactly one element of order two. For this purpose, we may assume the group to be $Z/2mZ$ under addition. Clearly m is the unique element of order two. Q.E.D.

From Lemma 2, we see that the prime power condition is only an illusory generalization of the prime condition. More precisely, $(\#)$ *is solvable for d prime if and only if $(\#)$ is solvable for d a power of prime.* This follows from the next result.

LEMMA 3. *Let p be an odd prime and k be a nonzero positive integer. Then* 2 *is of even order in* $(\mathbf{Z}/p\mathbf{Z})^*$ *if and only if* 2 *is of even order in* $(\mathbf{Z}/p^k\mathbf{Z})^*$.

Proof. The result is a particular instance of the following fact: x is of even order in $(\mathbf{Z}/p^k\mathbf{Z})^*$ if and only if $h(x)$ is of even order in $(\mathbf{Z}/p\mathbf{Z})^*$, where $h: \mathbf{Z}/p^k\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ is the epimorphism which reduces modulo p^k to modulo p. Sufficiency is obvious. For the necessity, assume x is of even order s, but $h(x)$ is of odd order t. Since $h(x^t) = 1$, so x^t is in the kernel of h, so x^t is of *odd* order, say t'. (The order of $(\mathbf{Z}/p^k\mathbf{Z})^*$ is $p^{k-1}(p-1)$ while that of $(\mathbf{Z}/p\mathbf{Z})^*$ is $p-1$. Hence kernel of h is of order p^{k-1}, which is *odd*.) Hence $x^{tt'} = 1$, which implies s divide tt', which is a contradiction because s is even but tt' is odd. Q.E.D.

Now we can state the main result.

THEOREM 4. *Let d be a power of an odd prime, so* $d \equiv 1, 3, 5, 7 \pmod 8$.

(a) *If* $d \equiv 1 \pmod 8$, *say* $d = 8n + 1$ *where* $n = 2^s t$ *with t odd, then* (#) *is solvable if and only if* $2^t \not\equiv 1 \pmod d$.

(b) *If* $d \equiv 3 \pmod 8$, *then* (#) *is solvable.*

(c) *If* $d \equiv 5 \pmod 8$, *then* (#) *is solvable.*

(d) *If* $d \equiv 7 \pmod 8$, *then* (#) *is not solvable.*

The proof rests upon the next lemma, which virtually drops out of two well-known facts concerning quadratic residue, namely, *Euler's criterion* and *Gauss' lemma*, the statements as well as proofs of which can be found in any standard text on elementary number theory (e.g., H. Davenport, *The Higher Arithmetic*, Hutchinson, London, 1952). For the sake of completeness we shall include here the proof of the lemma, which understandably would have to be an imitation of the proofs of the two aforementioned facts.

LEMMA 5. *Let p be a prime, then* $2^{\frac{1}{2}(p-1)} \equiv 1$ *or* $-1 \pmod p$ *according as* $p \equiv 1, 7 \pmod 8$ *or* $p \equiv 3, 5 \pmod 8$.

Proof. Write $(\mathbf{Z}/p\mathbf{Z})^* = \{1, 2, \cdots, p-1\} = \{\pm 1, \pm 2, \cdots, \pm \frac{1}{2}(p-1)\}$, then we see that

$$2 \cdot 4 \cdot 6 \cdots (p-1) = \begin{cases} (-1)(-3)\cdots(-\frac{1}{2}(p-3))(2)(4)\cdots(\frac{1}{2}(p-1)) & \text{if } \frac{1}{2}(p-1) \text{ even} \\ (-1)(-3)\cdots(-\frac{1}{2}(p-1))(2)(4)\cdots(\frac{1}{2}(p-3)) & \text{if } \frac{1}{2}(p-1) \text{ odd.} \end{cases}$$

In any case,

$$2^{\frac{1}{2}(p-1)} \cdot 1 \cdot 2 \cdots \tfrac{1}{2}(p-1) = (-1)^m \cdot 1 \cdot 2 \cdots \tfrac{1}{2}(p-1)$$

where m is the number of integers in $2, 4, 6, \cdots, p-1$ greater than $p/2$. It is not hard to check that m is even or odd according as $p \equiv 1, 7 \pmod 8$ or $p \equiv 3, 5 \pmod 8$. Since $2^{\frac{1}{2}(p-1)} = (-1)^m$, the result follows. Q.E.D.

Proof of Theorem 4. By the remark made after Lemma 2, we need only look at the case where d is a prime.

(a) If $2^t \equiv 1 \pmod{d}$, then r is odd, so (#) is not solvable. If $2^t \not\equiv 1 \pmod{d}$, then t cannot be a multiple of r, but $r \mid d-1 = 8n = 2^{3+s}t$, so r must be even, which implies (#) is solvable.

(b) and (c). Since $d \equiv 3, 5 \pmod{8}$ implies $2^{\frac{1}{2}(d-1)} \equiv -1 \pmod{d}$, then (#) is solvable.

(d) $d \equiv 7 \pmod{8}$ implies $2^{\frac{1}{2}(d-1)} \equiv 1 \pmod{d}$. But now $\frac{1}{2}(d-1)$ is odd, so r is odd, which implies (#) is not solvable. Q.E.D.

Naturally we like to know what happens in general. It is not hard to get a necessary condition. Namely, (#) is solvable only if all prime factors p of d are such that (#) is solvable for p. Unfortunately this is *not* a sufficient condition. For instance, (#) is solvable for 3 and 5, but *not* for 15. It would be interesting to see whether the following is true or false:

CONJECTURE 6. *(#) is solvable if and only if all prime factors p of d are such that (#) is solvable for p and all p are of the same type as categorized in Theorem* 4 (that is, all p are of the form described in (a), or all p are of the form described in (b), or all p are of the form described in (c)).

THE CLASSICAL RUIN PROBLEM WITH EQUAL INITIAL FORTUNES

S. M. SAMUELS, Purdue University

Let players A and B start with a and b dollars, respectively. Let them repeatedly toss a coin which has probability p of heads, $0 < p < 1$. Each time the coin comes up heads, A wins one dollar from B, while B wins a dollar from A if tails. The game continues until one of the players has no more money left (is "ruined"). What is the probability that ultimately A is ruined? What is the expected duration of the game?

This is the classical ruin problem and the answers to the above questions are very well known (Feller [1] pp. 344–349). Stern [2] recently showed that when $a = b$, the conditional expected durations of the game, given that A is ruined and given that B is ruined, are equal. Actually a stronger result is true, namely —

THEOREM. *If $a = b$, then the duration of the game is independent of who wins it.*

Proof. Assume $p \neq \frac{1}{2}$ since $p = \frac{1}{2}$ is trivial. Let $q = 1 - p$. Let D be the

Proof of Theorem 4. By the remark made after Lemma 2, we need only look at the case where d is a prime.

(a) If $2^t \equiv 1 \pmod d$, then r is odd, so (#) is not solvable. If $2^t \not\equiv 1 \pmod d$, then t cannot be a multiple of r, but $r \mid d-1 = 8n = 2^{3+s}t$, so r must be even, which implies (#) is solvable.

(b) and (c). Since $d \equiv 3, 5 \pmod 8$ implies $2^{\frac{1}{2}(d-1)} \equiv -1 \pmod d$, then (#) is solvable.

(d) $d \equiv 7 \pmod 8$ implies $2^{\frac{1}{2}(d-1)} \equiv 1 \pmod d$. But now $\frac{1}{2}(d-1)$ is odd, so r is odd, which implies (#) is not solvable. Q.E.D.

Naturally we like to know what happens in general. It is not hard to get a necessary condition. Namely, (#) is solvable only if all prime factors p of d are such that (#) is solvable for p. Unfortunately this is *not* a sufficient condition. For instance, (#) is solvable for 3 and 5, but *not* for 15. It would be interesting to see whether the following is true or false:

CONJECTURE 6. *(#) is solvable if and only if all prime factors p of d are such that (#) is solvable for p and all p are of the same type as categorized in Theorem* 4 (that is, all p are of the form described in (a), or all p are of the form described in (b), or all p are of the form described in (c)).

THE CLASSICAL RUIN PROBLEM WITH EQUAL INITIAL FORTUNES

S. M. SAMUELS, Purdue University

Let players A and B start with a and b dollars, respectively. Let them repeatedly toss a coin which has probability p of heads, $0 < p < 1$. Each time the coin comes up heads, A wins one dollar from B, while B wins a dollar from A if tails. The game continues until one of the players has no more money left (is "ruined"). What is the probability that ultimately A is ruined? What is the expected duration of the game?

This is the classical ruin problem and the answers to the above questions are very well known (Feller [1] pp. 344–349). Stern [2] recently showed that when $a = b$, the conditional expected durations of the game, given that A is ruined and given that B is ruined, are equal. Actually a stronger result is true, namely —

THEOREM. *If $a = b$, then the duration of the game is independent of who wins it.*

Proof. Assume $p \neq \frac{1}{2}$ since $p = \frac{1}{2}$ is trivial. Let $q = 1 - p$. Let D be the duration of the game and $W = 1$ if A wins, 0 if B wins. Of course independence of D and W is equivalent to *either* of the following:

(i) $P(D = d \mid W = 1) = P(D = d \mid W = 0)$ for all d,

(ii) $P(W = w \mid D = d) \equiv c(w)$ for $w = 0, 1$ and for all d such that $P(D = d) > 0$.

The latter is easy to prove: Let $A(d)$ and $B(d)$ be the sets of "all ways" in which A and B, respectively, are ruined in exactly d tosses. An element of $A(d)$ is a string of $(d + a)/2$ T's and $(d - a)/2$ H's arranged so that A is not ruined before there are d tosses. Now change the T's to H's and the H's to T's. The result is an element of $B(d)$. Thus it is easy to see that $A(d)$ and $B(d)$ each have the same number of elements and

$$P(B(d)) = (p/q)^a P(A(d)).$$

Hence

$$P(W = 0 \mid D = d) = P(A(d))/[P(A(d)) + P(B(d))] \equiv [1 + (p/q)^a]^{-1}$$

$$P(W = 1 \mid D = d) \equiv (p/q)^a \, [1 + (p/q)^a]^{-1}$$

for all d such that $P(D = d) > 0$, which proves the Theorem.

Of course $c(w)$ is the unconditional probability of A's ruin ($w = 0$) or B's ruin ($w = 1$), so, as a bonus, this proof provides a neat way of getting those probabilities when the initial fortunes are equal.

The theorem and the proof given here ought to be in print somewhere but I haven't been able to find them.

I think the proof given here takes some of the mystery out of the result as obtained by Stein. We see that whatever D is, the outcome is, in effect, some permutation of a "stand-off" for all but the last a tosses, these being then either all heads or all tails.

Notice that in proving the theorem, we have not found the common value of $P(D = d \mid W = 1)$ and $P(D = d \mid W = 0)$. But since they are equal for all d so are the conditional expectations and both are of course equal to the unconditional expectation, $E(D)$, which is easy to get by any of several familiar methods. One way is to look at the sequence

$$Y_n = X_n - n(p - q) \qquad n = 0, 1, 2, \cdots, D$$

where $X_0 = a$ and X_n is A's fortune after n tosses. It is easy to see that this is a bounded martingale, hence by a standard theorem,

$$E(Y_D) = E[X_D - D(p - q)] = EY_0 = a$$

so

$$E(D) = [E(X_D) - a]/(p - q)$$

where

$$E(X_D) = 2aP(W = 1).$$

(For the case $p = \frac{1}{2}$, use instead the martingale

$$Y_n = X_n^2 - n$$

to get $E(D) = a^2$.)

References

1. W. Feller, An Introduction to Probability Theory and its Applications vol. I, 3rd ed., Wiley, New York, 1968.
2. F. Stern, Conditional expectation of the duration in the classical ruin problem, this MAGAZINE, 48 (1975).

ON SUBSPACES OF SEPARABLE SPACES

DOUGLAS E. CAMERON, University of Akron

It is a well-known fact that separability is open hereditary (that is, open subspaces of separable spaces are separable) and hereditary in second countable spaces (all subspaces of a second countable space are separable). The purpose of this note is to show that the first result may be easily improved.

DEFINITION 1. *A subset A of a topological space (X, τ) is dense in X if* $\mathrm{cl}_\tau A = X$, *where* $\mathrm{cl}_\tau A$ *denotes the closure of A with respect to the topology τ.*

DEFINITION 2. *A topological space (X, τ) is separable if there is a countable dense subset of X.*

THEOREM 1. *Open subsets of separable spaces are separable.*

The standard proof involved here is to show that if D is a countable dense subset of X and A is open, then $D' = A \cap D$ is dense in A.

The preceding result may be improved as follows: For $B \subseteq X$, $C \subseteq B$, then $\mathrm{cl}_{\tau|B} C = \mathrm{cl}_\tau C \cap B$ where $\mathrm{cl}_{\tau|B} C$ is the closure of C in the relative topology on B.

If D' is a dense subset of A, $A \subseteq B \subseteq \mathrm{cl}_\tau A$, then $\mathrm{cl}_\tau D' \supseteq A$ and since $\mathrm{cl}_\tau D'$ is closed $\mathrm{cl}_\tau D' \supseteq \mathrm{cl}_\tau A$. Thus since $D' \subseteq A$, we have $\mathrm{cl}_\tau D' = \mathrm{cl}_\tau A$.

Therefore for $A \subseteq B \subseteq \mathrm{cl}_\tau A$, $\mathrm{cl}_{\tau|B} D' = (\mathrm{cl}_\tau D') \cap B = (\mathrm{cl}_\tau A) \cap B = B$. This may be summarized by stating

THEOREM 2. *If (X, τ) is a topological space, $A \subseteq X$ such that $(A, \tau | A)$ is separable, then $(B, \tau | B)$ is separable if $A \subseteq B \subseteq \mathrm{cl}_\tau A$.*

COROLLARY 1. *If (X, τ) is a separable space, then separability is inherited by all subsets B such that* $\mathrm{int}_\tau B \subseteq B \subseteq \mathrm{cl}_\tau(\mathrm{int}_\tau B)$ *where* $\mathrm{int}_\tau B$ *denotes the interior of B with respect to τ.*

DEFINITION 3. *A subset B of a topological space (X, τ) is regular closed if* $\mathrm{cl}_\tau(\mathrm{int}_\tau B) = B$.

COROLLARY 2. *Separability is inherited by regular closed sets.*

(For the case $p = \frac{1}{2}$, use instead the martingale

$$Y_n = X_n^2 - n$$

to get $E(D) = a^2$.)

References

1. W. Feller, An Introduction to Probability Theory and its Applications vol. I, 3rd ed., Wiley, New York, 1968.
2. F. Stern, Conditional expectation of the duration in the classical ruin problem, this MAGAZINE, 48 (1975).

ON SUBSPACES OF SEPARABLE SPACES

DOUGLAS E. CAMERON, University of Akron

It is a well-known fact that separability is open hereditary (that is, open subspaces of separable spaces are separable) and hereditary in second countable spaces (all subspaces of a second countable space are separable). The purpose of this note is to show that the first result may be easily improved.

DEFINITION 1. *A subset A of a topological space (X, τ) is dense in X if* $\mathrm{cl}_\tau A = X$, *where* $\mathrm{cl}_\tau A$ *denotes the closure of A with respect to the topology τ.*

DEFINITION 2. *A topological space (X, τ) is separable if there is a countable dense subset of X.*

THEOREM 1. *Open subsets of separable spaces are separable.*

The standard proof involved here is to show that if D is a countable dense subset of X and A is open, then $D' = A \cap D$ is dense in A.

The preceding result may be improved as follows: For $B \subseteq X$, $C \subseteq B$, then $\mathrm{cl}_{\tau|B} C = \mathrm{cl}_\tau C \cap B$ where $\mathrm{cl}_{\tau|B} C$ is the closure of C in the relative topology on B.

If D' is a dense subset of A, $A \subseteq B \subseteq \mathrm{cl}_\tau A$, then $\mathrm{cl}_\tau D' \supseteq A$ and since $\mathrm{cl}_\tau D'$ is closed $\mathrm{cl}_\tau D' \supseteq \mathrm{cl}_\tau A$. Thus since $D' \subseteq A$, we have $\mathrm{cl}_\tau D' = \mathrm{cl}_\tau A$.

Therefore for $A \subseteq B \subseteq \mathrm{cl}_\tau A$, $\mathrm{cl}_{\tau|B} D' = (\mathrm{cl}_\tau D') \cap B = (\mathrm{cl}_\tau A) \cap B = B$. This may be summarized by stating

THEOREM 2. *If (X, τ) is a topological space, $A \subseteq X$ such that $(A, \tau|A)$ is separable, then $(B, \tau|B)$ is separable if $A \subseteq B \subseteq \mathrm{cl}_\tau A$.*

COROLLARY 1. *If (X, τ) is a separable space, then separability is inherited by all subsets B such that* $\mathrm{int}_\tau B \subseteq B \subseteq \mathrm{cl}_\tau (\mathrm{int}_\tau B)$ *where* $\mathrm{int}_\tau B$ *denotes the interior of B with respect to τ.*

DEFINITION 3. *A subset B of a topological space (X, τ) is regular closed if* $\mathrm{cl}_\tau (\mathrm{int}_\tau B) = B$.

COROLLARY 2. *Separability is inherited by regular closed sets.*

ON POLYHEDRAL FACES

BENJAMIN L. SCHWARTZ, McLean, Virginia

Dedicated to David Silverman

Define two faces of a polyhedron as *compatible* if they have the same number of edges (or vertices). In this note, the following theorem is proved:

Every simply connected polyhedron has at least three pairs of compatible faces.

We require the convention that every vertex is incident to at least three faces. This precludes subdividing an edge. Otherwise we could, for example, transform a true triangle into a phony "quadrilateral" with two consective collinear edges. Such a figure would obviously not be a new polyhedron, but a different version of the old one.

The proof uses the Euler formula $E = V + F - 2$ and the following

LEMMA. *Let F_i denote the number of edges of face i. Then*

$$F - 2 \geqq (1/6) \sum F_i.$$

Proof. Every vertex is in at least three faces. Hence if we count vertices by face, every vertex will be counted at least three times, i.e., $3V \leqq \Sigma F_i$. Similarly, if we count edges by face, every edge is counted exactly twice: $2E = \Sigma F_i$. Combining these results

$$\tfrac{1}{2} \sum F_i = E = V + F - 2 \leqq (1/3) \sum F_i + F - 2,$$

from which the lemma follows at once. ∎

Now suppose there is a polyhedron with just two compatible face pairs. Since $F_i \geqq 3$, the minimum possible values for the F_i are

$$3, 3, 4, 4, 5, 6, 7, \cdots, F.$$

This is an arithmetic sequence with the first three terms modified. Hence

$$\sum F_i \geqq \tfrac{1}{2} F(F+1) + 4.$$

Combining this with the lemma, we get

$$F - 2 \geqq (1/6) \sum F_i \geqq (1/6)[\tfrac{1}{2} F(F+1) + 4],$$

or, upon simplifying slightly, $F^2 - 11F + 32 \leqq 0$. But this quadratic is positive definite, since the discriminant is negative. Thus the required inequality condition is never satisfied. The theorem follows. ∎

This proves that there are no polyhedra with less than three compatible face pairs. Figures 1 and 2 illustrate that there are polyhedra with exactly three pairs. It is left to the reader to show that these are the only figures with three pairs. In particular there is no polyhedron with a trio of compatible faces and no other compatible pairs.

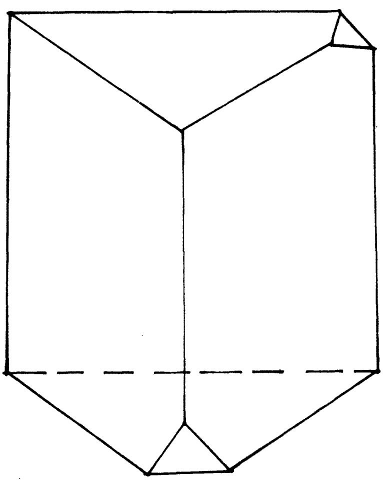


FIG. 1.

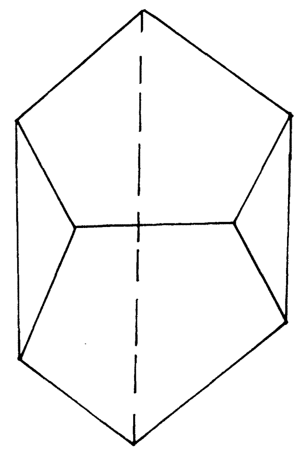


FIG. 2.

A CURIOUS SEQUENCE

STEVEN KAHAN, Queens College, Flushing, New York

Consider the sequence of k nonnegative integers $n_0, n_1, \cdots, n_{k-1}$, where n_i is the number of times that i appears in the sequence. For the sake of convenience, we will refer to such a sequence as a sequence of type (*) of order k. We make the initial observations that each $n_i \leqq k-1$ and that $k = \sum_{i=0}^{k-1} n_i$. In this paper, we prove part (a) of the following result, leaving the proof of part (b) to the reader.

THEOREM. (a) *If* $k \geqq 7$, *then a type* (*) *sequence of order* k *is uniquely determined and is given by* $n_0 = k-4$, $n_1 = 2$, $n_2 = 1$, $n_{k-4} = 1$, *and all other* $n_j = 0$.

(b) *If* $k < 7$, *then no type* (*) *sequence of order* k *exists for* $k = 1,2,3,6$; *there are two distinct type* (*) *sequences of order* 4: $n_0 = 1$, $n_1 = 2$, $n_2 = 1$, $n_3 = 0$ *and* $n_0 = 2$, $n_1 = 0$, $n_2 = 2$, $n_3 = 0$, *and a unique type* (*) *sequence of order* 5: $n_0 = 2$, $n_1 = 1$, $n_2 = 2$, $n_3 = 0$, $n_4 = 0$.

Proof of (a):

(1) $n_i \leqq 1$ for $i \geqq k-3$. For suppose $n_i > 1$ for some $i \geqq k-3$. Then some

pairs. Figures 1 and 2 illustrate that there are polyhedra with exactly three pairs. It is left to the reader to show that these are the only figures with three pairs. In particular there is no polyhedron with a trio of compatible faces and no other compatible pairs.

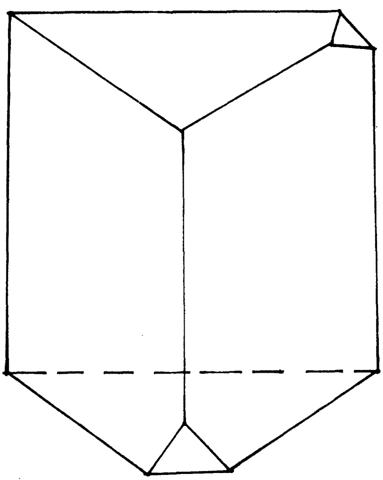


FIG. 1.

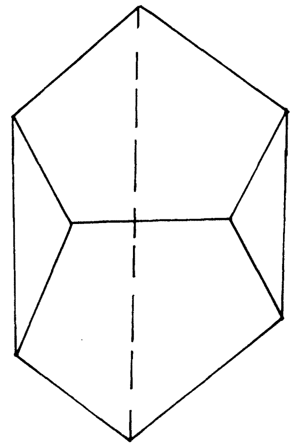


FIG. 2.

A CURIOUS SEQUENCE

STEVEN KAHAN, Queens College, Flushing, New York

Consider the sequence of k nonnegative integers $n_0, n_1, \cdots, n_{k-1}$, where n_i is the number of times that i appears in the sequence. For the sake of convenience, we will refer to such a sequence as a sequence of type (*) of order k. We make the initial observations that each $n_i \leqq k-1$ and that $k = \sum_{i=0}^{k-1} n_i$. In this paper, we prove part (a) of the following result, leaving the proof of part (b) to the reader.

THEOREM. (a) *If* $k \geqq 7$, *then a type* (*) *sequence of order* k *is uniquely determined and is given by* $n_0 = k-4$, $n_1 = 2$, $n_2 = 1$, $n_{k-4} = 1$, *and all other* $n_j = 0$.

(b) *If* $k < 7$, *then no type* (*) *sequence of order* k *exists for* $k = 1,2,3,6$; *there are two distinct type* (*) *sequences of order* 4: $n_0 = 1$, $n_1 = 2$, $n_2 = 1$, $n_3 = 0$ *and* $n_0 = 2$, $n_1 = 0$, $n_2 = 2$, $n_3 = 0$, *and a unique type* (*) *sequence of order* 5: $n_0 = 2$, $n_1 = 1$, $n_2 = 2$, $n_3 = 0$, $n_4 = 0$.

Proof of (a):

(1) $n_i \leqq 1$ for $i \geqq k-3$. For suppose $n_i > 1$ for some $i \geqq k-3$. Then some

number greater than or equal to $k-3$ appears at least twice in the sequence, so $k \geqq 2(k-3) = k + (k-6) > k$, a contradiction. The result follows.

(2) $n_{k-1} = 0$. Suppose $n_{k-1} = 1$. Then by definition, $k-1$ appears exactly once in the sequence, say at n_i. If $i \neq 1$, then since $n_1 \geqq 1$, we conclude that $k \geqq n_1 + n_i + n_{k-1} \geqq 1 + (k-1) + 1 = k+1$, a contradiction. So $n_1 = k-1$. Since $n_1 + n_{k-1} = k$, it follows that $n_0 = 0$, which is self-contradictory. Hence, $n_{k-1} \neq 1$. From (1), we conclude $n_{k-1} = 0$.

(3) $n_{k-2} = 0$. Suppose $n_{k-2} = 1$. Then by definition, $k-2$ appears exactly once in the sequence, say at n_i. Since $n_{k-2} = 1$, $n_1 \geqq 1$, and it is clear that $n_1 = 1$ would again be self-contradictory. So $n_1 \geqq 2$. If $i \neq 1$, then $k \geqq n_1 + n_i + n_{k-2} \geqq 2 + (k-2) + 1 = k+1$, a contradiction. Hence, $n_1 = k-2$, so 1 appears in the sequence $k-2$ times. Therefore, $k \geqq (k-2) + (k-2)(1) = 2k-4 = k + (k-4) > k$, a contradiction. It then follows that $n_{k-2} \neq 1$, and from (1) we may conclude that $n_{k-2} = 0$.

(4) $n_{k-3} = 0$. Suppose $n_{k-3} = 1$. Then by definition, $k-3$ appears exactly once in the sequence, say at n_i. Clearly, the only possible values of i are 0 and 1, since if $n_i = k-3$ for $i \geqq 2$, then i appears $k-3$ times in the sequence, and $k \geqq i(k-3) \geqq 2(k-3) = k + (k-6) > k$, a contradiction. So either $n_0 = k-3$ or $n_1 = k-3$. If the former, then as in (3), $n_1 \geqq 2$. Hence, to satisfy $\sum_{i=0}^{k-1} n_i = k$, it follows that $n_1 = 2$ and consequently $n_j = 0$ for $2 \leqq j \leqq k-1$, $j \neq k-3$. In particular, $n_2 = 0$, contradicting the fact that 2 appears in the sequence. So n_1 must equal $k-3$, which implies that 1 appears in the sequence $k-3$ times. But then $k \geqq (k-3) + (k-3)(1) = 2k-6 = k + (k-6) > k$, a contradiction. Therefore, $n_{k-3} \neq 1$, and it immediately follows from (1) that $n_{k-3} = 0$.

(5) $3 \leqq n_0 \leqq k-4$. The first part of the inequality is clear from (2), (3), and (4). To obtain the second part, observe that $n_0 = k-1$ implies $n_{k-1} \geqq 1$, contradicting (2); $n_0 = k-2$ implies $n_{k-2} \geqq 1$, contradicting (3); and $n_0 = k-3$ implies $n_{k-3} \geqq 1$, contradicting (4).

(6) $n_0 = k-4$. The result is obtained by induction on k. To begin, note that the result is a direct consequence of (5) for $k = 7$. Next, assume the result true for $k = m$, i.e., assume that for a type (*) sequence of order m, the first term is equal to $m-4$. Now consider $n_0, n_1, \cdots, n_m$, a type (*) sequence of order $m+1$. From (2), we already know that the last term, n_m, is equal to 0. Let $n_0 = i$, where from (5), $i \geqq 3$. If we focus on the first m terms of this sequence, we can derive a type (*) sequence of order m by subtracting 1 from n_0, subtracting 1 from n_i, and adding 1 to n_{i-1}. Then for this newly-obtained type (*) sequence of order m, the induction hypothesis guarantees that its first term is $m-4$, i.e., $i - 1 = m-4$. So $n_0 = i = (m+1) - 4$, proving the result for $k = m+1$ and thus completing the induction.

(7) $n_{k-4} = 1$. From (6), it is apparent that $n_{k-4} \geqq 1$. Suppose that $n_{k-4} > 2$. Then $k-4$ appears at least three times in the sequence, so $k \geqq 3(k-4) = k + (2k-12) > k$, a contradiction. So $n_{k-4} \leqq 2$. If $n_{k-4} = 2$, then $k-4$ appears twice and 2 appears at least once in the sequence, so $k \geqq 2(k-4) + 2 = 2k-6 = k + (k-6) > k$, a contradiction. So $n_{k-4} = 1$.

(8) $n_1 = 2$. From the fact that $\Sigma_{i=0}^{k-1} n_i = k$ and from (2), (3), (4), (6), and (7), we may immediately conclude that $\Sigma_{i=1}^{k-5} n_i = 3$. From (7), $n_1 \geqq 1$, and as in (3), $n_1 \neq 1$. Thus, $n_1 = 2$ or $n_1 = 3$. But if $n_1 = 3$, then necessarily $n_j = 0$, $2 \leqq j \leqq k-5$, so 0 appears $(k-6)+3 = k-3$ times in the sequence, contradicting (6). Therefore, $n_1 = 2$.

(9) $n_2 = 1$ and $n_j = 0$ for all other undetermined n_j, if any. From (8) and the the fact that $\Sigma_{i=1}^{k-5} n_i = 3$, it becomes clear that $\Sigma_{i=2}^{k-5} n_i = 1$. Therefore, one of these nonnegative integers must be 1 and the others, if any, must be 0. Again from (8), we see that 2 appears in the sequence. Hence, $n_2 = 1$ and $n_j = 0$ for all other undetermined n_j, if any.

NOTES AND COMMENTS

L. Carlitz notes the following typographical errors in his paper *A note on sums of three squares in* $GF[q,x]$ in the March 1975 issue:

p. 109, line 4^- should read:

$$arr_1 + bss_1 + ctt_1 = ar^2 - bs^2 + ct^2 = -2bs^2 \neq 0.$$

p. 109, line 2^- should read

$$r' = -\frac{r}{4bs^2}, \qquad s' = \frac{1}{4bs}, \qquad t' = -\frac{t}{4bs^2}.$$

Harold D. Shane comments on Nymann's *Generalization of the birthday problem* in the January 1975 issue as follows:

Nymann (p. 47) states, "...seems to show that it takes at least 254 people before the expected number of birthdays represented is 183." Actually, we have here the classical occupancy problem of placing n balls randomly in k receptacles. If we let X_n be the number of receptacles occupied, then $P(X_n = r)$ is well known (see, for example, Hoel, Port and Stone, *Introduction to Probability Theory*, p. 44). However, if we are interested only in expectations, there is a very neat trick available. Letting $E_n \doteq E(X_n)$, we may reason thus:

$$P\{X_{n+1} = x+1 \mid X_n = x\} = \frac{k-x}{k}, \quad P\{X_{n+1} = x \mid X_n = x\} = \frac{x}{k},$$

$$E\{X_{n+1} \mid X_n = x\} = (x+1)\cdot\frac{k-x}{k} + x\cdot\frac{x}{k} = 1 + x\frac{k-1}{k},$$

$$E_{n+1} = E\{X_{n+1}\} = E\{E[X_{n-1} \mid X_n]\} = 1 + E_n \cdot \frac{k-1}{k} \quad \text{and} \quad E_1 = 1.$$

The solution to this recurrence is $E_n = k[1-((k-1)/k)^n]$. For $E_n \geqq k/2$, $n \geqq \log 2/[\log k - \log(k-1)]$. If $k = 365$, $n \geqq 252.97$. Alternatively, to have $E_n = 183$,

$$n = \frac{\log 365 - \log 182}{\log 365 - \log 364} = 253.97.$$

(8) $n_1 = 2$. From the fact that $\Sigma_{i=0}^{k-1} n_i = k$ and from (2), (3), (4), (6), and (7), we may immediately conclude that $\Sigma_{i=1}^{k-5} n_i = 3$. From (7), $n_1 \geqq 1$, and as in (3), $n_1 \neq 1$. Thus, $n_1 = 2$ or $n_1 = 3$. But if $n_1 = 3$, then necessarily $n_j = 0$, $2 \leqq j \leqq k-5$, so 0 appears $(k-6)+3 = k-3$ times in the sequence, contradicting (6). Therefore, $n_1 = 2$.

(9) $n_2 = 1$ and $n_j = 0$ for all other undetermined n_j, if any. From (8) and the the fact that $\Sigma_{i=1}^{k-5} n_i = 3$, it becomes clear that $\Sigma_{i=2}^{k-5} n_i = 1$. Therefore, one of these nonnegative integers must be 1 and the others, if any, must be 0. Again from (8), we see that 2 appears in the sequence. Hence, $n_2 = 1$ and $n_j = 0$ for all other undetermined n_j, if any.

NOTES AND COMMENTS

L. Carlitz notes the following typographical errors in his paper *A note on sums of three squares in GF*$[q, x]$ in the March 1975 issue:

p. 109, line 4^- should read:

$$arr_1 + bss_1 + ctt_1 = ar^2 - bs^2 + ct^2 = -2bs^2 \neq 0.$$

p. 109, line 2^- should read

$$r' = -\frac{r}{4bs^2}, \qquad s' = \frac{1}{4bs}, \qquad t' = -\frac{t}{4bs^2}.$$

Harold D. Shane comments on Nymann's *Generalization of the birthday problem* in the January 1975 issue as follows:

Nymann (p. 47) states, "...seems to show that it takes at least 254 people before the expected number of birthdays represented is 183." Actually, we have here the classical occupancy problem of placing n balls randomly in k receptacles. If we let X_n be the number of receptacles occupied, then $P(X_n = r)$ is well known (see, for example, Hoel, Port and Stone, *Introduction to Probability Theory*, p. 44). However, if we are interested only in expectations, there is a very neat trick available. Letting $E_n \doteq E(X_n)$, we may reason thus:

$$P\{X_{n+1} = x+1 \mid X_n = x\} = \frac{k-x}{k}, \quad P\{X_{n+1} = x \mid X_n = x\} = \frac{x}{k},$$

$$E\{X_{n+1} \mid X_n = x\} = (x+1)\cdot\frac{k-x}{k} + x\cdot\frac{x}{k} = 1 + x\frac{k-1}{k},$$

$$E_{n+1} = E\{X_{n+1}\} = E\{E[X_{n-1} \mid X_n]\} = 1 + E_n \cdot \frac{k-1}{k} \quad \text{and} \quad E_1 = 1.$$

The solution to this recurrence is $E_n = k[1-((k-1)/k)^n]$. For $E_n \geqq k/2$, $n \geqq \log 2/[\log k - \log(k-1)]$. If $k = 365$, $n \geqq 252.97$. Alternatively, to have $E_n = 183$,

$$n = \frac{\log 365 - \log 182}{\log 365 - \log 364} = 253.97.$$

PROBLEMS AND SOLUTIONS

Readers of this department are invited to submit for solution problems believed to be new that may arise in study, in research, or in extra-academic situations. Problems may be submitted fron any branch of mathematics and ranging in subject content from that accessible to the talented high school student to problems challenging to the professional mathematician. Proposals should be accompanied by solutions, when available, and by any information that will assist the editor. Ordinarily, problems in well-known textbooks should not be submitted.

The asterisk (*) will be placed by the problem number to indicate that the proposer did not supply a solution. Readers' solutions are solicited for all problems. Proposers' solutions may not be "best possible" and solutions by others will be given preference.

Solutions should be submitted on separate, signed sheets. Figures should be drawn in India ink, and exactly the size desired for reproduction.

Send all communications for this department to Dan Eustice, the Ohio State University, 231 W. 18th Ave., Columbus, Ohio 43210.

To be considered for publication, solutions should be mailed before June 1, 1976.

PROPOSALS

954. *Proposed by Richard L. Francis, Southeast Missouri State University.*

Show that any even perfect number greater than 28 can be represented as the sum of at least two perfect numbers.

955. *Proposed by Charles F. White, Oxon Hill, Maryland.*

For three line segments of unequal lengths a, b, and c drawn on a plane from a common point, characterize the proper angular positions such that the outer end-points of the line segments define the maximum-area triangle. Show how to approximate the exact values of the angles for $a = 3$, $b = 4$, and $c = 5$.

956. *Proposed by Arthur Marshall, Madison, Wisconsin.*

Let Q_m be the product of the first m primes: $Q_2 = 6$, $Q_3 = 30$, etc. Then, for $m \geqq 2$, $Q_m/2$ is the product of the first $m-1$ *odd* primes. Now $Q_2/2 = 2^1 + 1 = 2^2 - 1$, while $Q_3/2 = 2^4 - 1$. For $m > 3$, can $Q_m/2 = 2^j \pm 1$ for integer j?

957. *Proposed by Erwin Just, Bronx Community College.*

Show that it is possible to partition the rational points of the plane into four sets, each of which is dense in the plane, and such that no straight line will contain a point from each of the four sets.

*Can the partitioning also be into three sets?

958. *Proposed by Murray S. Klamkin, University of Waterloo.*

Give direct proofs of the following two results:

a. If $\mathrm{Re}(z_0) > 0$ and the sequence $\{z_n\}$ is defined for $n \geqq 1$ by

$$z_n = \frac{1}{2}\left(z_{n-1} + \frac{A}{z_{n-1}}\right),$$

where A is real and positive, then $\mathrm{limit}_{n\to\infty} z_n = \sqrt{A}$.

b. Suppose $\{x_n\}$ is a real sequence defined for $n \geqq 1$ by

$$x_n = \frac{1}{2}\left(x_{n-1} - \frac{A}{x_{n-1}}\right),$$

where A is positive. Show that if p is a given integer greater than 1, then the initial term x_0 can be chosen so that $\{x_n\}$ is periodic with period p. (These results are contained implicitly in K. E. Hirst, *A square root algorithm giving periodic sequences*, J. London Math. Soc., (2) 6 (1972) 56–60.)

959. *Proposed by L. Carlitz, Duke University.*

Let P be a point in the interior of the triangle ABC and let r_1, r_2, r_3 denote the distances from P to the sides of the triangle. Let R denote the circumradius of ABC. Show that

$$\sqrt{r_1} + \sqrt{r_2} + \sqrt{r_3} \leqq 3\sqrt{R/2},$$

with equality if and only if ABC is equilateral and P is the center of ABC.

960. *Proposed by Alan Wayne, Pasco-Hernando Community College, Florida.*

In a rectangle of dimensions a and b, lines parallel to the sides divide the interior into ab square unit areas. Through the interior of how many of these unit squares will a diagonal of the rectangle pass?

*Can the result be generalized to higher dimensions?

961. *Proposed by Erwin Schmid, Washington, D.C.*

The sequence $11^0, 11^1, 11^2, \cdots$ of integral powers of the number 11, reduced modulo 50, i.e., $1, 11, 21, 31, 41, 1, \cdots \pmod{50}$ is in both geometric and arithmetic progression. What is the law of formation for such series?

962. *Proposed by Curt Monash, The Ohio State University.*

Consider the space curve, $C(t)$, defined by $C(t) = (t^k, t^m, t^n)$ for $t \geqq 0$ and k, m, and n, integers.

a. Show that if (k, m, n) equals $(1, 2, 3)$ or $(-2, -1, 1)$, then $C(t)$ does not contain four coplanar points.

b. Show that for $(k, m, n) = (1, 3, 4)$, $C(t)$ does contain four coplanar points.

c*. Find a characterization of (k, m, n) so that $C(t)$ does not contain four coplanar points.

QUICKIES

From time to time this department will publish problems which may be solved by laborious methods, but which with the proper insight may be disposed of with dispatch. Readers are urged to submit their favorite problems of this type, together with the elegant solution and the source, if known.

Q628. If [ ] denotes the greatest integer function, derive a formula for $\Sigma_{k=1}^{m}[kn/m]$ in terms of m, n, and $d=(m,n)$, the greatest common divisor of m and n.

[*Submitted by Brother Alfred Brousseau*]

Q629. Show that $\Sigma_{k=1}^{\infty}\tan^{-1}(1/(2k^2))=\pi/4$.

[*Submitted by Norman Schaumberger*]

Q630. Suppose a skew quadrilateral $ABCD$, with diagonal AC perpendicular to diagonal BD, is transformed into the quadrilateral $A'B'C'D'$ so that the corresponding lengths of the sides are preserved. Prove that $A'C'$ is perpendicular to $B'D'$.

[*Submitted by M. S. Klamkin and M. Sayrafiezadeh*]

(Answers on pages 302–303)

SOLUTIONS

Bracket Function Equality

915. [November, 1974] *Proposed by Jerome H. Manheim, Bradley University, Peoria, Illinois.*

For arbitrary k and p show the bracket function satisfies

$$\left[\frac{10^k-p}{p}\right]+\left[\frac{-(10^k+1)}{p}\right]+2=0.$$

Editor's comment. The proposer's original intention was that k and p be positive integers. Since many readers went beyond, thereby finding a counterexample, we have selected two different approaches to the original statement.

I. *Solution by D. P. Choudhury, Kanpur, India.*

There is nothing sacred about 10^k and we shall prove in general that $[(x-p)/p]+[-(x+1)/p]=-2$ for any positive integers x and p.

Let $x=ap+b$ with $0\leqq b<p$. Then,

$$\left[\frac{x}{p}-1\right]+\left[-\frac{(x+1)}{p}\right]=\left[\frac{x}{p}\right]-1+\left[-\frac{(x+1)}{p}\right]=a+\left[-\frac{(ap+b+1)}{p}\right]-1$$

$$=a+\left[-\frac{(b+1)}{p}\right]-a-1=\left[-\frac{(b+1)}{p}\right]-1=-2.$$

II. *Solution by N. J. Kuenzi and John Oman, University of Wisconsin-Oshkosh.*

Since the given equation does not hold for arbitrary real numbers k and p, under what conditions or restrictions on k and p will the equation hold? To answer this question let us consider two cases, $p>0$ and $p<0$.

Suppose that $p>0$ and $n=[(10^k-p)/p]$. It follows that $n+1\leqq 10^k/p<n+2$, $0<p(n+2)-10^k$, and $n+1<(10^k+1)/p$. If $n+1<(10^k+1)/p\leqq n+2$ then $[-(10^k+1)/p]=-(n+2)$. Since $10^k/p<n+2$, $(10^k+1)/p\leqq n+2$ whenever $1/p\leqq n+2-10^k/p$ or, equivalently, $1\leqq p(n+2)-10^k$. However, if $0<p(n+2)-10^k<1$, then $-(10^k+1)/p<-(n+2)$, $[-(10^k+1)/p]\leqq -(n+3)$, and $[(10^k-p)/p]+[-(10^k+1)/p]+2\leqq n-(n+3)+2=-1$. So for $p>0$ and $n=[(10^k-p)/p]$, $[(10^k-p)/p]+[-(10^k+1)/p]+2=0$ if and only if $1\leqq p(n+2)-10^k$. We might note that if k and p are arbitrary positive integers then the equation will hold because $0<p(n+2)-10^k$ forces the condition $1\leqq p(n+2)-10^k$.

Suppose that $p<0$ and $n=[(10^k-p)/p]$. It follows that $n+1\leqq 10^k/p<n+2$, $p(n+1)-10^k\geqq 0$, and $(10^k+1)/p<n+2$. If $n+1<(10^k+1)/p\leqq n+2$ then $[-(10^k+1)/p]=-(n+2)$. Since $n+1\leqq 10^k/p<n+2$ and $p<0$, $n+1<(10^k+1)/p<n+2$ whenever $p(n+1)-10^k>1$. However, if $0\leqq p(n+1)-10^k\leqq 1$, then $-(n+1)\leqq -(10^k+1)/p$, $[-(10^k+1)/p]\geqq -(n+1)$, and $[(10^k-p)/p]+[-(10^k+1)/p]+2\geqq n-(n+1)+2=1$. So for $p<0$ and $n=[(10^k-p)/p]$, $[(10^k-p)/p]+[-(10^k+1)/p]+2=0$ if and only if $p(n+1)-10^k>1$. In this case we note that if p and k are negative integers and $p\neq -1$, the condition $p(n+1)-10^k>1$ is satisfied.

Also solved by Alfred Brousseau, Arthur Cooke, Thomas Elsner, Jay Folkert, Leon Gerber, M. G. Greening (Australia), Heiko Harborth (West Germany), Robert Hashway, M. S. Klamkin (Canada), Vaclav Konecny (Czechoslovakia), Lew Kowarski, James McHutchion, Joseph V. Michalowicz, Marilyn Rodeen, Davis Stone, Eric Sturley, Edward T. H. Wang (Canada), Kenneth Wilke, and the proposer.

Trilinear Coordinates

916. [November, 1974] *Proposed by H. Demir, M.E.T.U., Ankara, Turkey.*

Let XYZ be the pedal triangle of a point P with regard to the triangle ABC. Then find the trilinear coordinates x, y, z of P such that

$$YA+AZ=ZB+BX=XC+CY.$$

Solution by M. S. Klamkin, University of Waterloo.

By drawing segments from P parallel to AB and AC respectively and terminating on BC, it follows that

$$BX = x \cot B + z \csc B, \qquad CX = x \cot C + y \csc C.$$

The other distances CY, AY, AZ, BZ follow by cyclic interchange. From the hypothesis,

$$(y+z)(\cot A + \csc A) = (z+x)(\cot B + \csc B) = (x+y)(\cot C + \csc C) = \frac{2s}{3}$$

where s = semiperimeter. Solving:

$$x = \frac{s}{3}\left(\tan\frac{B}{2} + \tan\frac{C}{2} - \tan\frac{A}{2}\right),$$

$$y = \frac{s}{3}\left(\tan\frac{A}{2} + \tan\frac{C}{2} - \tan\frac{B}{2}\right),$$

and

$$z = \frac{s}{3}\left(\tan\frac{A}{2} + \tan\frac{B}{2} - \tan\frac{C}{2}\right).$$

Also solved by D. M. Bailey, Gordon Bennett, Alfred Brousseau, Michael Goldberg, J. M. Stark, and the proposer.

Rotating Faces

917. [November, 1974] *Proposed by Charles W. Trigg, San Diego, California.*

The length of every edge of a regular pentagonal prism is e.

(a) When the two pentagonal faces are rotated about parallel diagonals until two of their edges coincide, two lateral edges vanish and one becomes elongated. The resulting hexahedron has two congruent regular pentagons, two congruent equilateral triangles, and two congruent trapezoids for faces. Eleven of its edges are equal. What is the length of the twelfth edge?

(b) When the pentagonal faces are otherwise rotated about the parallel diagonals until two of the vertices coincide, one lateral edge vanishes and two are elongated. The resulting heptahedron has two congruent regular pentagons, two congruent equilateral triangles, two congruent trapezoids and one rectangle for faces. Twelve of its edges are equal. What are the lengths of the other two edges?

Solution by J. W. Wilson, Gaithersberg, Maryland.

Take the cross-section of the regular pentagonal prism such that the cross-section is the perpendicular bisector of the parallel diagonals about which the respective rotations will be done. This cross-section is a rectangle of width e and with length corresponding to an altitude of the pentagon. Further this length is divided into two parts by the intersection with the diagonals of the pentagon. It is well known that the diagonals of a pentagon cut each other into two parts giving the golden ratio and also that a diagonal therefore divides an altitude in the same ratio.

During either of the rotations, the two points of intersection of the cross-section with the diagonals remain fixed, a distance e apart, and the rectangular cross-section is deformed into an isosceles triangle with the length of the base being the desired lengths of edges to be found in the problem.

For (a), the triangular cross-section has the two equal sides of the isosceles triangle divided into two parts in the golden ratio such that the larger part is adjacent to the vertex; for (b) the smaller part is adjacent to the vertex. Using similar triangles, the desired length in (a) is Ge, where G is the golden ratio $(1+\sqrt{5})/2$ and the desired length in (b) is $(1+G)e$; or $((1+\sqrt{5})/2)e$ and $((3+\sqrt{5})/2)e$, respectively.

Also solved by Michael Goldberg, Mike Keith, Lawrence A. Ringenberg, Marilyn Rodeen, Brian Smithgall, Sam Zaslavsky, and the proposer.

A Recurrence Relation

918. [November, 1974] *Proposed by Erwin Just, Bronx Community College.*

Let F_n be the nth member of the sequence defined by $F_n = F_{n-2} + F_{n-3}$, with $F_1 = 1$, $F_2 = 0$, $F_3 = 1$. Prove that $F_{2n} - F_{n-1}^2$ is divisible by F_n.

Solution by Leonard Carlitz, Duke University.

We first show that

$$(*) \qquad F_m = F_{k+1}F_{m-k} + F_{k+2}F_{m-k-1} + F_kF_{m-k-2},$$

where $k \geqq 0$ and $F_0 = 0$.

By the given recurrence,

$$F_m = 1\cdot F_m + 0\cdot F_{m-1} + 0\cdot F_{m-2} = 0\cdot F_{m-1} + 1\cdot F_{m-2} + 1\cdot F_{m-3}$$
$$= 1\cdot F_{m-2} + 1\cdot F_{m-3} + 0\cdot F_{m-4}.$$

Since $F_0 = 0$, $F_1 = 1$, $F_2 = 0$, $F_3 = 1$, and $F_4 = 1$, it follows that $(*)$ holds for $k = 0, 1, 2$. Assuming that $(*)$ holds for values up to and including k, we have

$$F_m = F_{k+1}(F_{m-k-2} + F_{m-k-3}) + F_{k+2}F_{m-k-1} + F_kF_{m-k-2}$$
$$= F_{k+2}F_{m-k-1} + (F_{k+1} + F_k)F_{m-k-2} + F_{k+1}F_{m-k-3}$$
$$= F_{k+2}F_{m-k-1} + F_{k+3}F_{m-k-2} + F_{k+1}F_{m-k-3}.$$

Hence $(*)$ holds for all $k \geqq 0$. If we take $m = 2n$ and $k = n-1$ in $(*)$, we get

$$F_{2n} = F_nF_{n+1} + F_{n+1}F_n + F_{n-1}F_{n-1},$$

so that $F_{2n} - F_{n-1}^2 = 2F_nF_{n+1}$, yielding result.

REMARK. If we take $m = 2n+1$ and $k = n$ in $(*)$, we get

$$F_{2n+1} = F_{n+1}F_{n+1} + F_{n+2}F_n + F_nF_{n-1},$$

so that

$$F_{2n+1} - F_{n+1}^2 = F_n(F_{n+2} + F_{n-1}).$$

Hence, we also have that F_n divides $F_{2n+1} - F_{n+1}^2$.

Also solved by Gerald Bergum, George Berzsenyi, Walter Bluger (Canada), Alfred Brousseau, D. P. Choudhury (India), F. B. Correia, Clayton W. Dodge, M. G. Greening (Australia), Heiko Harborth (West Germany), M. S. Krishnamoorthy (India), N. J. Kuenzi & Bob Prielipp, Graham Lord, K. L. McAvaney (Australia), John Oman, F. D. Parker, N. Pastides, C. B. A. Peck, A. G. Shannon (Australia), David R. Stone, L. Van Hamme (Belgium), Kenneth Wilke, and the proposer.

N. Pastides derives relation $(*)$ of the solution from the more general recurrence relation $F_n = F_{n-3} + xF_{n-2}$, where x is a real number, and also proves a converse of the result.

A Simplex with Orthogonal Edges

919. [November, 1974] *Proposed by M. S. Klamkin, Ford Motor Company.*

An $(n+1)$-dimensional simplex with vertices $O, A_1, A_2, \cdots, A_{n+1}$ is such that the $(n+1)$ concurrent edges OA_i are mutually orthogonal. Show that the orthogonal projection of O onto the n-dimensional face opposite to it coincides with the orthocenter of that face (this generalizes the known result for $n = 2$).

Solution by Leon Gerber, St. John's University.

Let O be the origin of an $(n+1)$-dimensional coordinate system and let A_i lie on the ith coordinate axis at a distance a_i from O. The equation of the face F opposite O is $\Sigma_{i=1}^{n+1} x_i/a_i = 1$. Let $a^{-1} = \Sigma_{i=1}^{n+1} a_i^{-2}$ and let $H = (a/a_i)$. Clearly H lies in F and OH is perpendicular to F. Also,

$$A_1H \cdot A_2A_3 = [a/a_1 - a_1, a/a_2, a/a_3, \cdots, a/a_{n+1}] \cdot [0, -a_2, a_3, 0, \cdots, 0]$$
$$= -a + a = 0,$$

so A_1H is perpendicular to A_2A_3, and similarly for any three distinct subscripts.

REMARK. This result and its converse, namely that if an n-simplex is orthocentric there exist numbers a_i, $i = 1, \ldots, n+1$ such that $A_iA_j^2 = a_i^2 + a_j^2$, $i \neq j$, is in the literature:

W. J. C. Sharp, On the properties of simplicissima, Proc. London Math. Soc., (1886–7) 325–359 (footnote on p. 358).

E. Egervary, On orthocentric simplexes, Acta Litt. Sci. Szeged, 9 (1940) 218–226.

Also solved by M. G. Greening (Australia), and the proposer.

Radius of Nine-Point Circle

920. [November, 1974] *Proposed by Leon Bankoff, Los Angeles, California.*

If r, r_1, r_2, r_3 are the inradius and ex-radii of a triangle and h_1, h_2, h_3 are the altitudes, show that the radius of the nine-point circle is equal to $rr_1r_2r_3/h_1h_2h_3$.

Solution by Ragnar Dybvik, Tingvoll, Norway.

From the formulas

$$\frac{1}{h_1}=\frac{a_1}{2\Delta}, \quad \frac{a_1a_2a_3}{\Delta}=4R \quad \text{and} \quad \Delta^2=rr_1r_2r_3$$

where Δ is the area of the triangle, a_1, a_2 and a_3 the lengths of the sides and R the radius of the circumcircle (see Roger A. Johnson: *Advanced Euclidean Geometry*, pages 189 and 190), we easily get $rr_1r_2r_3/h_1h_2h_3 = R/2 =$ the radius of the nine-point circle.

Also solved by D. M. Bailey, Gordon Bennett, L. Carlitz, Clayton W. Dodge, Howard Eves, Alex G. Ferrer (Mexico), Leon Gerber, George Gruber, S. L. Haven & J. M. Stark, M. S. Klamkin, Graham Lord, U. V. Mallikharjunarao (India), Alan Wayne, and the proposer.

Euler's Phi

921. [November, 1974] *Proposed by Heiko Harborth, TU Braunschweig, Germany.*

Determine all integers n with $n = a^b/[\phi(a^b)-(\phi(a))^b]$, where a and b are positive integers, and $\phi(m)$ is Euler's totient function.

Solution by Richard A. Gibbs, Fort Lewis College.

Let $a = \Pi_{i=1}^N p_i^{e_i}$ where p_i are distinct primes. Then, setting $k = \Pi_{i=1}^N ((p_i-1)/p_i)$, it follows, from product formula for $\phi(a)$, that $n = 1/(k-k^b)$ or $nk^b - nk + 1 = 0$. Since k must be a rational root, $k = 1/n'$ where $n' \mid n$. Thus $n = (n')^b/((n')^{b-1}-1)$ and $(n')^{b-1}-1 = 1$, since $((n')^{b-1}-1, (n')^b) = 1$. Therefore, $(n')^{b-1} = 2$ so that $n' = b = 2$ and $n = 4$.

(We remark that $n' = 2$ implies $N = 1$ and $p_1 = 2$ and therefore the solution is obtained whenever a is any power of 2 and $b = 2$.)

Also solved by Alfred Brousseau, D. P. Choudhury (India), Steven P. Galovich, M. G. Greening (Australia), Lew Kowarski, Barry W. Light, Graham Lord, T. E. Moore, Bob Prielipp, David R. Stone, Eric Sturley, Kenneth M. Wilke, and the proposer.

Comments

1. Belatedly we acknowledge the solvers of the following problems:

879 W. Lorsin; **880** Jeffrey Baumwell, Lew Kowarski, and Alan Wayne; **888** D. P. Choudhury and Lee Hagglund; **889** Kathy Belie, D. P. Choudhury, C. T.

Haskell, and Alan Wayne; **893** D. P. Choudhury, F. D. Parker, and Alan Wayne; **894** C. W. Trigg and Kevin Upton; **895** Frederick Gray; **896** C. W. Trigg; **906** D. P. Choudhury.

Some solvers of Problems **880–886** were somehow acknowledged in the September, 1974 issue.

2. C. W. Trigg, C. C. Oursler, and R. Cormier & J. L. Selfridge have sent calculations on Problem **886** [November, 1973] for which we had received only partial results [January, 1975].

Given an initial positive integer N_0, define $N_{k+1} = 1 + N_k + S_k$, where S_k is the sum of the distinct prime, proper divisors of N_k. Doug Engel had conjectured that, for every initial integer N_0, the sequence $\{N_k\}$ merges with the sequence formed when $N_0 = 1$.

Cormier and Selfridge sent the following results:

There appear to be five sequences beginning with integers less than 1000 which do not merge. These sequences were carried out to 100,000,000 or more. The calculations are:

1, 2, 3, 4, 7, 8, $\cdots\cdots\cdots\cdots\cdots$, 96,532,994, 144,799,494, $\cdots$(31)

393, 528, 545, 660, 682, 727, $\cdots\cdots\cdot$, 97,622,612, 122,028,268, $\cdots$(9)

412, 518, 565, 684, 709, 710, $\cdots\cdots\cdot$, 92,029,059, 102,254,514, $\cdots$(46)

668, 838, 1260, 1278, 1355, 1632, $\cdots\cdot$, 91,127,590, 100,240,357, $\cdots$(52)

932, 1168, 1244, 1558, 1621, 1622, $\cdots$, 98,457,737, 112,523,136, $\cdots$(30)

The numbers in parentheses show the number of terms between 50,000,000 and 100,000,000. The rate of growth of these sequences suggests that there are likely an infinite number of mutually independent sequences.

3. Problem **882** [C. W. Trigg, November, 1973] involved finding a magic square with positive prime elements, six of which are the same as those in the magic square

101	5	71
29	59	89
47	113	17

The answer was published in the January, 1975 issue. We feel that some readers would like to see the reasoning leading to the unique solution. The following argument is due to Kenneth M. Wilke.

Since each prime element in the given square is of the form $6k+5$, we can derive it from the magic square whose elements are the corresponding values of k (Figure 1). These elements can be arranged in a square so as to form arithmetic progressions both horizontally and vertically. In Figure 2, $a = 0$, $d = 2$, and $c = 7$. Now we seek new values of a, c, and d so that three new arithmetic progressions of the same type are formed and so that six elements in the new progressions are the same as those in Figure 1 and the remaining three will generate primes of the form $6k+5$. Since all nine numbers of the form $a+id+jc$, where both i and j run through the values 0, 1 and 2, must generate primes of the form $6k+5$, none can be a multiple of five unless $a=0$ and this yields only the square of Figure 1. A check of the least positive residues (mod 5) yields the unique solution $a=4$, $d=2$, and $c=5$. This generates the magic square of Figure 3.

16	0	11
4	9	14
7	18	2

FIG. 1.

a	$a+d$	$a+2d$
$a+c$	$a+c+d$	$a+c+2d$
$a+2c$	$a+2c+d$	$a+2c+2d$

FIG. 2.

101	29	83
53	71	89
59	113	41

FIG. 3.

In addition to solving the original problem, two readers found related 'almost'-prime magic squares. C. W. Trigg found the magic square in Figure 4 and B. G. Hoerbelt found the magic square in Figure 5 which has seven of the original primes as elements.

143	89	71
29	101	173
131	113	59

FIG. 4.

89	17	71
41	59	77
47	101	29

FIG. 5.

ANSWERS

A628. Consider a right triangle in the plane with right angle at the origin and base m and height n on the coordinate axes. The given summation represents the number of lattice points in the triangle excluding the lattice points on the base. By Pick's theorem, $B/2+I-1=A$, where B is the number of boundary lattice points, I is the number of interior lattice points, and A is the area. Hence, we have $(m+n+d)/2+I-1=mn/2$. Solving for I, we find

$$\sum_{k=1}^{m}\left[\frac{kn}{m}\right]=\frac{(m-1)(n-1)-d+1}{2}+n+d-1=\frac{mn+n-m+d}{2}.$$

A629. From the formula for the tangent of the difference of two angles, we find that

$$\tan^{-1}\frac{1}{2k-1}-\tan^{-1}\frac{1}{2k+1}=\tan^{-1}\frac{1}{2k^2}.$$

Summing, we have

$$\sum_{k=1}^{n} \tan^{-1} \frac{1}{2k^2} = \tan^{-1} 1 - \tan^{-1} \frac{1}{2n+1} = \frac{\pi}{4} - \tan^{-1} \frac{1}{2n+1}.$$

Upon letting $n \to \infty$, the result follows.

A630. The result is a consequence of the following, which is elementary but apparently not widely known:

THEOREM. *Given vectors a, b, c, and d such that $a + b + c + d = 0$, then $(a + b)$ is perpendicular to $(a + d)$ if and only if $|a|^2 + |c|^2 = |b|^2 + |d|^2$.*

Proof. Using dot products,

$$c \cdot c = (-1)^2(d + a + b) \cdot (d + a + b) = |a|^2 + |b|^2 + |d|^2 + 2(a \cdot b + a \cdot d + d \cdot b)$$
$$= |b|^2 + |d|^2 - |a|^2 + 2(a \cdot a + a \cdot b + a \cdot d + d \cdot b).$$

Hence,

$$|a|^2 + |c|^2 = |b|^2 + |d|^2 + 2(a + b) \cdot (a + d),$$

and the theorem follows.

Note. A more geometric proof can be given by considering spheres centered at some of the vertices of the figures and the powers of certain points with respect to them.

(Quickies on page 295)

ACKNOWLEDGEMENT

The editors wish to thank the following mathematicians for their assistance in refereeing manuscripts submitted to the MATHEMATICS MAGAZINE: T. Apostol, F. Bagemihl, E. Beckenbach, L. Beinecke, E. Burniston, G. Chartrand, L. Cote, D. Drasin, M. Drazin, U. Dudley, C. Goffman, D. Gottlieb, H. Gould, E. Grosswald, P. Hagis, V. Hoggatt, R. Holmes, J. Huneycutt, N. Kazarinoff, M. Klamkin, E. Lippa, G. Ludden, R. Lynch, H. Pollard, J. Riordan, J. Rubin, S. Samuels, E. Schenkman, A. Schwenk, J. Selfridge, C. Trigg, J. Tweed, C. Vanden Eynden, S. Weingram, A. Wilansky, M. Wunderlich, J. Yackel, E. Zachmanoglou, R. Zink.

WILEY'S GOT YOUR NUMBER.

Whatever your Introductory
Mathematics course number,
whatever that course covers, there's a
Wiley text to help you teach it
more effectively, easily. Here are 7.

The World-Renowned

NEW MATHEMATICAL LIBRARY

is now published by

THE MATHEMATICAL ASSOCIATION OF AMERICA

This continuing series of inexpensive, paperbound books by mathematical scholars is designed for the high school or college student who wants a new challenge in understanding and appreciating important mathematical concepts. Internationally acclaimed as the most distinguished series of its kind, the NEW MATHEMATICAL LIBRARY features eminent expositors Ross Honsberger, Ivan Niven, H.S.M. Coxeter, and others of equal stature. Another distinctive feature of NML is its collection of problem books from high school mathematical competitions in the U.S. and abroad. Teachers at all levels will find many stimulating ideas in these books suitable for the classroom or independent study. The books are ideal for supplementary reading, school libraries, advanced or honor students, mathematics clubs, or the teacher's professional library. *Watch for new titles that will appear regularly.*

NUMBERS: RATIONAL AND IRRATIONAL (NML-01)
by Ivan Niven.
A clear interesting exposition of number systems, beginning with the natural numbers and extending to the rational and real numbers.

WHAT IS CALCULUS ABOUT? (NML-02)
by W. W. Sawyer
Develops the basic concepts of calculus intuitively, exploiting such familiar concepts as speed, acceleration, and volume.

AN INTRODUCTION TO INEQUALITIES (NML-03)
by E. F. Beckenbach and R. Bellman
Includes an axiomatic treatment of inequalities, proofs of the classical inequalities and powerful applications to optimum problems.

GEOMETRIC INEQUALITIES (NML-04)
by N. D. Kazarinoff
An informal presentation of the arithmetic mean-geometric mean inequality and discussions of the famous isoperimetric theorems, the reflection principle, and Steiner's symmetrization—with problem solving emphasis.

THE CONTEST PROBLEM BOOK (NML-05)
Problems from the Annual High School Mathematics Contests sponsored by the MAA and four other organizations. Covers the period 1950-1960. Compiled and with solutions by Charles T. Salkind.
A complete collection of examination questions and solutions from the first decade of this national high school mathematics competition. No mathematics beyond intermediate algebra required. Elementary procedures are consistently used in solutions, but more sophisticated alternatives are included where appropriate.

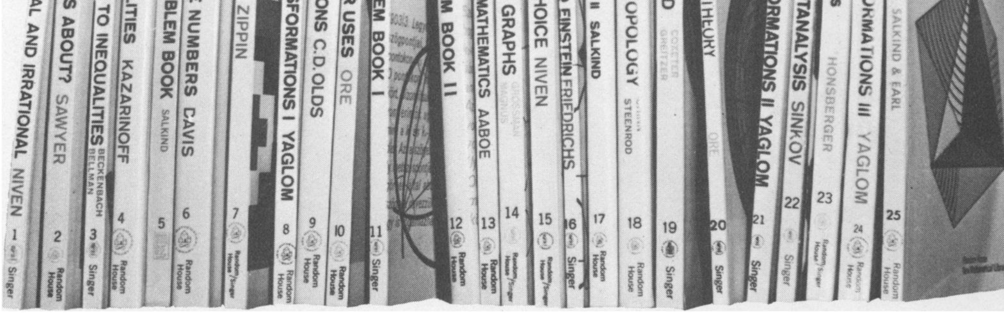
THE LORE OF LARGE NUMBERS (NML-06)
by P. J. Davis
How to work with numbers, big and small, and understand some of their less obvious properties.

USES OF INFINITY (NML-07)
by Leo Zippin
How mathematics have transformed the almost mystic concept of infinity into a precise tool essential in all branches of mathematics.

GEOMETRIC TRANSFORMATIONS (NML-08)
by I. M. Yaglom translated by Allen Shields
Concerned with isometries (distance-preserving transformations), a completely different way of looking at familiar geometrical facts that supplies the students with methods by which powerful problem solving techniques may be developed.

CONTINUED FRACTIONS (NML-09)
by Carl D. Olds
Shows how rational fractions can be expanded into continued fractions and introduces such diverse topics as the solutions of linear Diophantine equations, expansion of irrational numbers into infinite continued fractions and rational approximation to irrational numbers.

GRAPHS AND THEIR USES (NML-10)
by Oystein Ore
Develops enough graph theory to approach such problems as scheduling the games of a baseball league or a chess tournament, solving some ancient puzzles or analyzing winning (or losing) positions in certain games.



HUNGARIAN PROBLEM BOOK I (NML-11)
HUNGARIAN PROBLEM BOOK II (NML-12)
Based on the Eötvös Competitions 1894-1928
translated by E. Rapaport
The challenging problems that have become famous for the simplicity of the concepts employed, the mathematical depth reached, and the diversity of elementary mathematical fields touched.

EPISODES FROM THE EARLY HISTORY OF MATHEMATICS (NML-13)
by A. Aaboe
The contributions and amazing progress made by ancient mathematicians are revealed as the author describes Babylonian arithmetic and topics reconstructed from *Eculid's Elements;* from the writings of Archimedes and from Ptolemy's *Almagest.*

GROUPS AND THEIR GRAPHS (NML-14)
by I. Grossman and W. Magnus
In this introduction to group theory, abstract groups are made concrete in visual patterns that correspond to group structure. Suitable for students at a relatively early stage of mathematical growth.

THE MATHEMATICS OF CHOICE (NML-15)
by Ivan Niven
Stresses combinatorial mathematics and a variety of ingenious methods for solving questions about counting. Offers preparation for the study of probability.

FROM PYTHAGORAS TO EINSTEIN (NML-16)
by K. O. Friedrichs
The Pythagorean theorem and the basic facts of vector geometry are discussed in a variety of mathematical and physical contexts leading to the famous $E = mc^2$.

THE MAA PROBLEM BOOK II (NML-17)
A continuation of NML 5 containing problems and solutions from the Annual High School Mathematics Contests for the period 1961-1965.

FIRST CONCEPTS OF TOPOLOGY (NML-18)
by W. G. Chinn and N. E. Steenrod
The development of topology and some of its simple applications. The power and adaptability of topology are demonstrated in proving so-called existence theorems.

GEOMETRY REVISITED (NML-19)
by H.S.M. Coxeter and S. L. Greitzer
The purpose of this book is to revisit elementary geometry, using modern techniques such as transformations, inversive geometry, and projective geometry to facilitate geometric understanding and link the subject with other branches of mathematics.

INVITATION TO NUMBER THEORY (NML-20)
by Oystein Ore
A highly readable introduction to number theory that explains why the properties of numbers have always held such fascination for man. Problems, with solutions, allow students to find number relationships of their own.

GEOMETRIC TRANSFORMATIONS II (NML-21)
by I. M. Yaglom translated by Allen Shields
Similarity (shape-preserving) transformations are dealt with in the same manner in which distance-preserving transformations were treated in the first volume in *Geometric Transformations* (NML-8). Includes numerous problems with detailed solutions.

ELEMENTARY CRYPTANALYSIS — A Mathematical Approach (NML-22)
by Abraham Sinkov
In this systematic introduction to the mathematical aspects of cryptography, the author discusses monoalphabetic and polyalphabetic substitutions, digraphic ciphers and transpositions. The necessary mathematical tools include modular arithmetic, linear algebra of two dimensions with matrices, combinatorics and statistics. Each topic is developed as needed to solve decoding problems.

INGENUITY IN MATHEMATICS (NML-23)
by Ross Honsberger
Nineteen independent essays that reveal elegant and ingenious approaches used in thinking about such topics in elementary mathematics as number theory, geometry, combinatorics, logic and probability.

GEOMETRIC TRANSFORMATIONS III (NML-24)
by I. M. Yaglom translated by Abe Shenitzer
This part of Yaglom's work (sequel to NML-08 and NML-21) treats affine and projective transformations, and introduces the reader to non-Euclidean geometry in a supplement to hyperbolic geometry. As in the previously published parts of his work, Yaglom focuses on problems and their detailed solutions and keeps the text brief and simple.

THE MAA PROBLEM BOOK III (NML-25)
A continuation of NML-05 and NML-17, containing problems and solutions from the Annual High School Mathematics Contests for the period 1966-1972.

MATHEMATICS MAGAZINE, Vol. 48, No. 5, NOVEMBER-DECEMBER 1975