MATHEMATICS MAGAZINE

CONTENTS

VOLUME 42 • JANUARY 1969 • NUMBER 1

MATHEMATICS MAGAZINE

STEPHEN A. JENNINGS, *EDITOR*

EDITORIAL CORRESPONDENCE should be sent to the EDITOR, S. A. JENNINGS, Department of Mathematics, University of Victoria, Victoria, British Columbia, Canada. Articles should be typewritten and double-spaced on $8\frac{1}{2}$ by 11 paper. The greatest possible care should be taken in preparing the manuscript, and authors should keep a complete copy. Figures should be drawn on separate sheets in India ink and of a suitable size for photographing.

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: 1 year $4.00 Members of the Mathematical Association of America and of Mu Alpha Theta may subscribe at the special rate of 2 years for $6.00. Single copies are 80¢.

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

MM

MATHEMATICS MAGAZINE

Published by

THE MATHEMATICAL ASSOCIATION OF AMERICA
(INCORPORATED)

A JOURNAL
OF COLLEGIATE MATHEMATICS

VOLUME 42
1969

Published at

MENASHA, WIS., AND WASHINGTON, D. C.

A WORD FROM THE NEW EDITOR

With this issue, I take over as Editor of the MATHEMATICS MAGAZINE from Roy Dubisch, and I am happy to be able to express to him, on behalf of all readers, our thanks for his efforts on our behalf over the past five years. I myself can only hope that during the coming five years I succeed in strengthening this Magazine as much as he has.

Readers need not anticipate sudden changes in editorial policy, for the pattern of the MATHEMATICS MAGAZINE is now well established. Our continued success will depend, as it has in the past, on expository and critical articles both from previous contributors and especially from new authors. If you have an idea for an article, and are not sure whether the topic or treatment is appropriate, may I suggest that you write to me? I would also welcome comments, criticisms and suggestions from all readers.

S. A. JENNINGS, University of Victoria

TANGENTS: AN ELEMENTARY SURVEY

HUGH THURSTON, University of British Columbia, Vancouver

1. Tangents in antiquity. The concept of tangent must have been in men's minds from very early times, but the first clear statements about tangents were those made by the classical Greek geometers. Even Euclid, however, gave no *definition* of tangent: a tangent to him was simply a line which touches a curve; and "touch" is a nontechnical word.

The first result which he proves ([1] Book 3, Proposition 16) is: The straight line drawn at right angles to the diameter of a circle from its extremity will fall outside the circle; and into the space between the straight line and the circumference no other straight line can be interposed.

The proposition finishes: From this it is manifest that the straight line drawn at right angles to the diameter of a circle from its extremity touches the circle. Thus the definition of tangent implicit in Euclid's *Elements* is that it is a line with two properties:

(i) It has one point in common with the circle, and all the other points are outside, and

(ii) it is impossible to interpose another line "between" it and the curve.

The same definition is implicit in the works of Apollonius on conics and of Archimedes on the spiral. With the spiral, however, a significant new factor arises. Archimedes states ([2] Proposition 13): "If a straight line touch the spiral, it will touch it in one point only." However, what he proves is that it

A WORD FROM THE NEW EDITOR

With this issue, I take over as Editor of the MATHEMATICS MAGAZINE from Roy Dubisch, and I am happy to be able to express to him, on behalf of all readers, our thanks for his efforts on our behalf over the past five years. I myself can only hope that during the coming five years I succeed in strengthening this Magazine as much as he has.

Readers need not anticipate sudden changes in editorial policy, for the pattern of the MATHEMATICS MAGAZINE is now well established. Our continued success will depend, as it has in the past, on expository and critical articles both from previous contributors and especially from new authors. If you have an idea for an article, and are not sure whether the topic or treatment is appropriate, may I suggest that you write to me? I would also welcome comments, criticisms and suggestions from all readers.

S. A. JENNINGS, University of Victoria

TANGENTS: AN ELEMENTARY SURVEY

HUGH THURSTON, University of British Columbia, Vancouver

1. Tangents in antiquity. The concept of tangent must have been in men's minds from very early times, but the first clear statements about tangents were those made by the classical Greek geometers. Even Euclid, however, gave no *definition* of tangent: a tangent to him was simply a line which touches a curve; and "touch" is a nontechnical word.

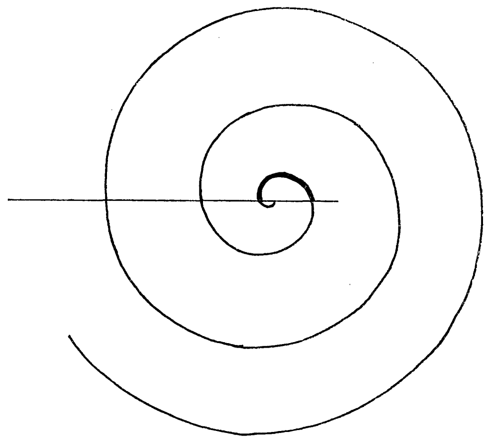
The first result which he proves ([1] Book 3, Proposition 16) is: The straight line drawn at right angles to the diameter of a circle from its extremity will fall outside the circle; and into the space between the straight line and the circumference no other straight line can be interposed.

The proposition finishes: From this it is manifest that the straight line drawn at right angles to the diameter of a circle from its extremity touches the circle. Thus the definition of tangent implicit in Euclid's *Elements* is that it is a line with two properties:

(i) It has one point in common with the circle, and all the other points are outside, and

(ii) it is impossible to interpose another line "between" it and the curve.

The same definition is implicit in the works of Apollonius on conics and of Archimedes on the spiral. With the spiral, however, a significant new factor arises. Archimedes states ([2] Proposition 13): "If a straight line touch the spiral, it will touch it in one point only." However, what he proves is that it



DIAG. 1

does not touch the same half-turn of the spiral twice: in Diagram 1, for instance, no line touches the thickened part of the spiral at two points. (The proof used only the first of the two properties (i) and (ii) described above.) The new factor is that the tangent is now seen to be a *local* concept: the important part of the tangent-line at P to a curve is a small segment containing P in its interior—the rest of the line is of no importance.

Behind part (i) of the definition of tangent mentioned above lies the concept of what we should nowadays call a *support-line*: "move a ruler up to a penny until it touches it, and then it is a tangent." At a sharp corner of a curve there may be support-lines, but part (ii) of the definition shows that Euclid would not have called such a support-line a tangent.

2. The tangent and the derivative. Every reader will know that the tangent to a graph at a given point is the line through that point whose slope is the value of the derivative there. No doubt this result was first accepted with only informal definitions of derivative and of tangent. Eventually a good definition of derivative was devised, and then the question arose of devising a good definition of tangent. Perhaps the definition that we inferred above from Euclid could have been used,—certainly it is not hard to show that the line whose slope is the derivative is the only one with property (ii) of that definition—but instead mathematicians devised a new definition of tangent strongly inspired by the definition of derivative: namely, the tangent at P to a curve is the limit of the secant PQ as Q tends to P along the curve. Once made, this definition is seen to apply to curves in space as well as to plane curves. When this definition is analyzed it becomes:

The line L is a tangent at the point P to the curve S if P lies on both L and S and if, for each positive ϵ, there is a sphere with center P such that every point of S inside the sphere is inside a (double) cone with vertex P, axis L, and vertical angle ϵ.

It is then easy to prove that if S is the graph of a function F, and P is the point on S with abscissa a, then S has a nonvertical tangent at P if and only if $F'(a)$ exists, and that $F'(a)$ is the slope of the tangent. Thus the concepts of tangent and derivative are closely allied.

Some treatments try to exploit this alliance by actually defining the tangent in terms of the derivative. However, a definition on the lines of "The tangent to the curve $y=F(x)$ at the point P with abscissa a is the line through P with slope $F'(a)$ if $F'(a)$ exists, and is the vertical line through P if $[F(a+h)-F(a)]/h$ tends to ∞ (or to $-\infty$) as h tends to zero" is not logical. The reason is that it defines *tangent* in terms of a particular system of coordinates. If a plane curve is given we can set up cartesian coordinates in its plane, find its equation, and use the definition to find the tangent at P. We can then set up different axes in the plane, find the equation of the curve referred to them, and use our definition to find the tangent. We have no guarantee that the two tangents we have found will be the same. Not until invariance under change of axes has been proved can the definition be accepted as a valid definition of "tangent": until then it is only a definition of "tangent with respect to a given system of coordinates."

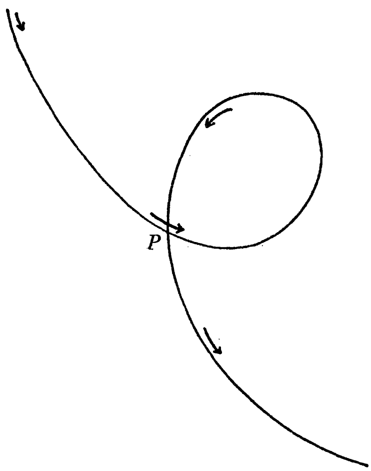
The definition also lacks generality. Few plane curves can be put in the form $y=F(x)$. However, many plane curves are *locally* of the form $y=F(x)$ for suitable axes. Thus the definition could be saved by being modified as follows: *If P is a point on a plane curve S, and if there is a circle with center P such that, in a given system of cartesian coordinates, the part of S inside the circle coincides with the part of the graph of $y=F(x)$ inside the circle, and P has abscissa a, and $F'(a)$ exists; then the line through P with slope $F'(a)$ is a tangent at P to S with respect to the given system of coordinates.* It is then not hard to prove that the tangent is independent of the choice of F, and that two systems of cartesian coordinates cannot yield two different tangents. Then if there is a tangent at P with respect to any one system of coordinates we call it the tangent at P *tout court.*

This definition will cover the common elementary plane curves, but still lacks complete generality, as we shall see in Section 5. The reader may by now be thinking that there is little point in a definition of tangent to a curve which leaves the equally difficult concept of curve undefined. But happily, it turns out that no matter how curve is defined, provided only that it is defined as some set of points, our definition holds. To show this, we frame the definition of tangent to apply quite generally to sets of points. We have to ensure that P is not an isolated point of the set; the rest is easy.

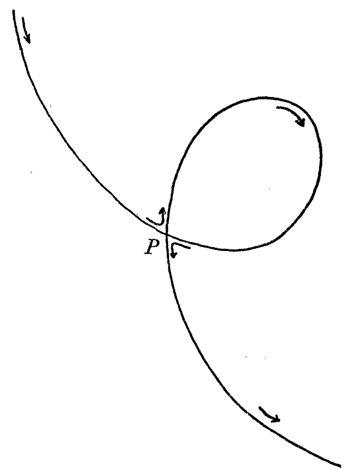
DEFINITION. *The line L is a tangent at P to the set S if P lies on L and belongs to S and if, for each positive ϵ, there is a sphere with center P such that (i) every point of S inside the sphere is inside a (double) cone with vertex P, axis L, and vertical angle ϵ and* (ii) *there is at least one point of S, other than P, whose distance from P is less than ϵ.*

This is the definition of tangent to a curve which we shall use throughout this article. It is clear that there is at most *one* tangent to S at P; and that if S is a plane set, all tangents must lie in its plane. When convenient (in diagrams, for instance) we shall unblushingly restrict ourselves to the plane.

3. A dynamical approach. With the rise of dynamical astronomy from Galileo's time onward, curves and tangents began to be regarded in a different light. An ellipse now was known not merely as the set of points in which a cone is cut by a certain plane, but also as the path of a heavenly body. In general, a natural definition of a curve is that it is the path of a continuously-moving particle, and the tangent at a point P is the direction-of-motion of the particle when it is at P. The earliest specific statement of this which I can find was made by Roberval in 1730: "*La direction du mouvement d'un point qui décrit une ligne courbe est la touchante de la ligne courbe en chaque position de ce point là*" [3].



DIAG. 2



DIAG. 3

This definition, though natural, leads to several complications. The first is that a path is by no means the same thing as a curve in the old sense: Diagrams 2 and 3 show the same curve, but different paths. A *path* has a parametrization

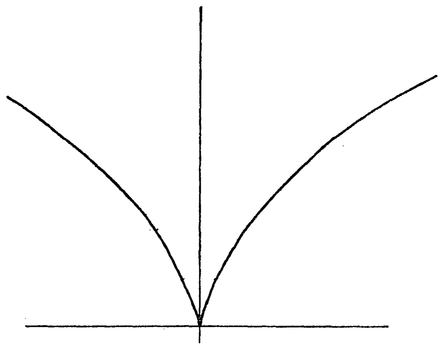
$$x = X(t), \qquad y = Y(t)$$

(which, if t denotes time, is the equation-of-motion of the particle traversing the path); the set of image-points under this mapping is a *curve*. However, it would not be satisfactory to define a path to *be* a parametrization: two different parametrizations which carry the image-point round the curve in Diagram 2 following the arrows should yield the same path. Thus a path could be defined very informally as a curve with arrows, or more formally as an equivalence-class of parametrizations. It is not too difficult to specify a suitable equivalence.

Some writers use the word "curve" in the sense in which we have been using "path." What we have called a curve is to them the *trace* of a curve.

In our terminology, given a system of cartesian coordinates in a plane, the unit circle with center at the origin is a curve, S say. *S traversed once anticlockwise* is a path, P_1. *S traversed twice clockwise* is a different path, P_2, with the same trace, namely the curve S.

The difference between a curve and a path makes itself felt when we consider tangents at a double point. A good definition of tangent to a *path* would clearly allow two tangents at P in Diagram 2, none in Diagram 3. There are, on our definition, no tangents at P to the curve shown in these diagrams. There is, however, a tangent at the origin to the curve shown in Diagram 4.



DIAG. 4 $x=t^3$, $y=t^2$.

We are left, then, with a definition of a (plane) curve as the trace of a parametrization.

$$x = X(t), \qquad y = Y(t), \qquad t \in T$$

where T is an interval, and X and Y are continuous on T. This definition seemed satisfactory until Peano proved that it implies that a square is a curve.

4. Simple arcs. Both the difficulties mentioned at the end of Section 3 are caused by points with more than one parameter. For instance, the point P on the curve in Diagrams 2 and 3 must, in any parametrization, have at least two parameters.

Let us call a parametrization of a curve *simple* if no points of the curve have more than one parameter. A curve which has a simple parametrization of the form

$$x = X(t), \qquad y = Y(t), \qquad a \leqq t \leqq b$$

is a *simple arc*. It will, of course, have infinitely many other simple parametrizations, as well as infinitely many nonsimple parametrizations. However, for a simple arc, only the simple parametrizations are of any great interest.

A square has no simple parametrization, and so is not a simple arc. In fact, it is known (see [**4**]) that a set is a simple arc if and only if it is closed, bounded, and connected, and the removal of any of its points, with two exceptions, will disconnect it. (The two exceptions are, of course, the end-points.)

If we restrict our attention to simple arcs we shall avoid the complications due to points with multiple parameters, but will still leave ourselves plenty of interesting material.

5. Tangents to a simple arc. The technique for finding the tangent to the arc given by the simple parametrization

$$x = X(t), \qquad y = Y(t)$$

at the point P with parameter p is well known in elementary calculus: if the ratio $X'(p): Y'(p)$ exists, then the line through P with direction ratio

$$X'(p): Y'(p)$$

is the required tangent. (This fact can be strictly proved on our definition of tangent: see [5] Theorem 13.) If $X'(p)$ and $Y'(p)$ are both zero, their ratio does not exist, and we seek another parametrization.

Two questions arise naturally. The first is: Is this technique more general than the one implied in Section 2, namely choosing axes so that our arc is locally of the form $y = F(x)$? (That technique is, of course, equivalent to choosing x as parametric variable.) The answer is "yes": an arc can be found with the following properties:

(i) It has a simple parametrization $x = X(t)$, $y = Y(t)$ in which the origin has parameter 0;

(ii) $X'(0): Y'(0)$ exists;

(iii) Under no change of axes is the arc locally of the form $y = F(x)$ at the point in question. The parametrization is

$$X(t) = t^2 \cdot \sin t^{-1} + \tfrac{1}{2}t \quad \text{if } 0 < |t| \leqq 1, \; X(0) = 0.$$
$$Y(t) = t \cdot X(t).$$

The details are in [5] Section 18. The secret is, of course, that for the curve *not* to be locally of the form $y = F(x)$, the equation $x = X(t)$ must not be locally solvable for t. Nevertheless, the derivative must exist at our point and be nonzero. X is in fact the well known function of G. H. Hardy ([6] Section 125) which has a nonzero derivative without local monotonicity.

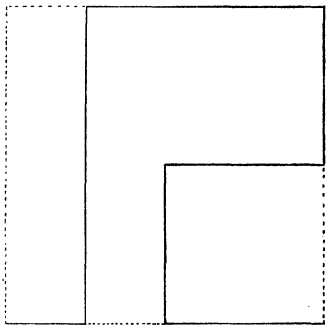
This is the result which we had in mind when, at the end of Section 2, we pointed out that the definition proposed there lacked generality.

The second question about the technique of the present paragraph is: Is it completely general? That is to say, if it is known that a tangent to a given simple arc at a given point P exists, can we always find a simple parametrization $x = X(t)$, $y = Y(t)$ of the arc for which the ratio $X'(p): Y'(p)$ exists, where p is the parameter of P? The answer—no—was given by G. Valiron in 1927 [8] and by A. J. Ward in 1937 [7].

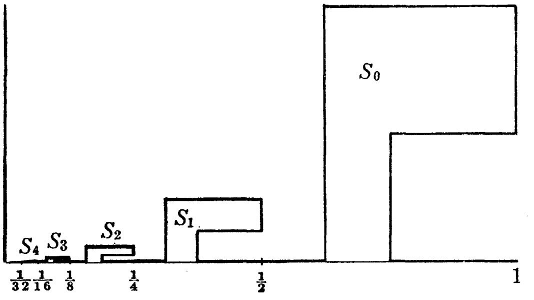
The arc which Ward used is based on the Greek-key pattern shown in Diagram 5, in which the corners are supposed to be rounded off by small quadrants. I use a slightly simplified arc. A scale copy S_0 of the pattern is placed on the segment $[1/2, 1]$ of the x-axis as shown in Diagram 6. S_0 is then copied at half scale and when this has been done the vertical scale is halved again. The result, S_1, is placed on the segment $[1/4, 1/2]$. S_1 is treated in the same way and the result, S_2, is placed on the segment $[1/8, 1/4]$, and in this way S_n is defined for every positive integer n. Finally the segment $[-1, 0]$ is drawn. The union of the points on all these arcs is clearly a simple arc, and equally clearly the x-axis is the tangent at the origin.

Now let

$$x = X(t), \qquad y = Y(t), \qquad a \leqq t \leqq b$$

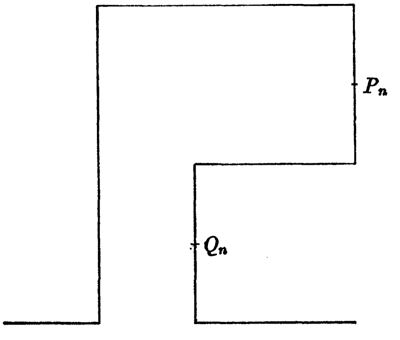


DIAG. 5



DIAG. 6

by any simple parametrization of the arc. Let us suppose that $(-1, 0)$ has parameter a and $(1, 0)$ has parameter b; similar arguments will hold for parametrizations running in the opposite direction. Let p be the parameter of the origin. Ward proved that if $X'(p)$ exists, then it must be zero. The proof goes as follows. Let P_n and Q_n be the points on S_n shown in Diagram 7, and let their parameters be u_n and v_n. Then $\{u_n\}$ and $\{v_n\}$ are sequences converging to p.



DIAG. 7

Therefore if $X'(p)$ exists, then both

$$\frac{X(u_n) - X(p)}{u_n - p}$$

and

$$\frac{X(v_n) - X(p)}{v_n - p}$$

must converge to $X'(p)$.
However,

$X(u_n)$, the abscissa of P_n, is 2^{-n}

$X(v_n)$, the abscissa of Q_n, is $(3/4) \times 2^{-n}$

$X(p)$, the abscissa of the origin, is 0.

Thus

$$X(u_n) - X(p) = \frac{4}{3}\{X(v_n) - X(p)\}.$$

Also

$$v_n - p > u_n - p$$

because P_n lies between the origin and Q_n on the arc. Therefore

$$\frac{X(u_n) - X(p)}{u_n - p} > \frac{4}{3}\,\frac{X(v_n) - X(p)}{v_n - p}$$

Therefore $X'(p) \geqq \frac{4}{3}X'(p)$. Clearly $X'(p) \geqq 0$. Therefore $X'(p) = 0$.

Now if $Y'(p)$ exists it cannot be nonzero, for then the y-axis would be the tangent at the origin. Thus if $X'(p)$ and $Y'(p)$ both exist, they must both be zero.

6. Cusps. On our definition of tangent, a curve has a tangent at a cusp. Some readers may find this slightly surprising because the familiar definition in terms of the derivative mentioned in Section 2 does not allow tangents at cusps (the mention of infinite derivatives there was only to allow tangents at points like the origin on $y = x^{1/3}$). The familiar definition could no doubt have been modified to allow tangents at cusps, but from many points of view it would be better to bridge the gap from the other side—to modify our definition to disallow tangent at cusps.

There are several arguments in favor of this course. One is that common sense does not suggest that the line $x = 0$ is a tangent in Diagram 4, but rather that the ray $x = 0$, $y > 0$ is a semitangent. Indeed, if the concept of tangent is founded on the concept of direction-of-motion, we should certainly not want to allow a tangent where the direction-of-motion does not merely change abruptly, but actually reverses itself. Further, when we consider continuity of tangent-direction, we see that allowing tangents at cusps allows some unnatural complications. Arcs with continuously-turning tangents may not have certain properties which we should expect of a reasonably well-behaved curve: the properties of rectifiability, of regularity (the "arc over chord tends to 1" property) and of having smooth parametrizations. (A parametrization $x = X(t)$, $y = Y(t)$ is smooth if X' and Y' are continuous, and $X'(t)$ and $Y'(t)$ are never both zero.)

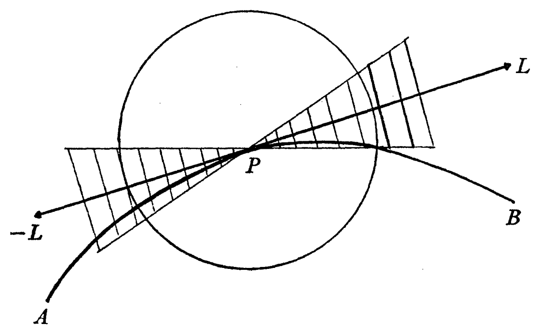
These considerations, especially those in the second paragraph of the section, suggest that we might define a tangent not as a line but as a directed line.

7. Directed tangents. Although it is possible to define order on a simple arc by purely topological means, the simplest method is to use a parametrization. If, on the arc given by the simple parametrization

$$x = X(t), \qquad y = Y(t), \qquad a \leqq t \leqq b,$$

the points A, B, P, Q have parameters a, b, p, q respectively, we say that Q is between B and P (and P between A and Q) with respect to this parametrization if $p<q$. Then, as can easily be proved, Q is between B and P with respect to any simple parametrization of the arc; and we say that Q is between B and P on the arc.

Our definition of directed tangent is as follows. Let P be a point on a simple arc S with end-points A, B; and let L be a directed line through P. Then L is a directed tangent to S at P (in the sense from A to B) if, for each positive ϵ, there is a sphere with center P such that every point of S between B and P which is inside the sphere is also inside the (single) cone with vertex, P, axis, L, and vertical angle ϵ, and every point of S between A and P which is inside the sphere is also inside the cone with vertex P, axis $-L$, and vertical angle ϵ. (See Diagram 8.)



DIAG. 8

Clearly $-L$ is then a directed tangent to S at P in the sense from B to A. It follows easily that if

$$x = X(t), \qquad y = Y(t), \qquad a \leqq t \leqq b$$

is a simple parametrization of the arc S, in which a is the parameter of A and b of B and if P is the point with parameter p, where $a<p<b$, and if

$$\frac{X(t) - X(p)}{\{[X(t) - X(p)]^2 + [Y(t) - Y(p)]^2\}^{1/2}} \to \begin{cases} l \text{ as } t \to p+ \\ -l \text{ as } t \to p- \end{cases}$$

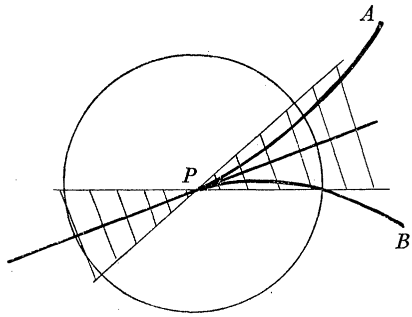
and

$$\frac{Y(t) - Y(p)}{\{[X(t) - X(p)]^2 + [Y(t) - Y(p)]^2\}^{1/2}} \to \begin{cases} m \text{ as } t \to p+ \\ -m \text{ as } t \to p- \end{cases}$$

then $l^2+m^2=1$ and the directed line through P with direction-cosines l, m is the directed tangent to S at P in the sense from A to B.

It is clear that wherever the directed tangent exists, the (undirected) line coinciding with it will be the tangent. On the other hand, although the tangent will exist at a cusp, the directed tangent will not (see Diagram 9).

We can define a directed semitangent at the end-point of an arc in the obvious way.



DIAG. 9

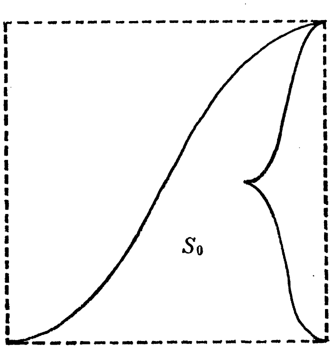
Directed tangents seem to have been first investigated by G. Valiron in 1927 [8]. A treatment of the three-dimensional case is included in T. M. Flett's paper [9] from which (corollary to Theorem 8) we obtain the following results:

If the directed tangent at the point P with parameter p exists, and if its direction-cosines are continuous there, then the arc-length TP exists wherever the parameter t of T is near enough to P and

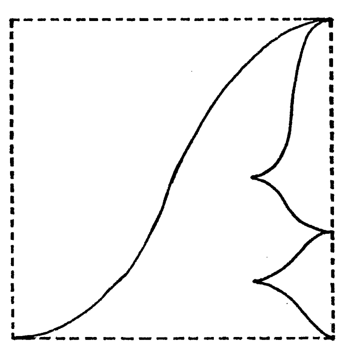
$$\frac{\text{arc-length } TP}{TP} \to 1 \quad \text{as} \quad t \to p.$$

If the directed tangent exists and its direction-cosines are continuous at each point of S, then S is rectifiable. Moreover, with arc-length as parametric variable, the arc is smooth.

These results, which follow from the existence of a continuously-turning *directed* tangent, by no means follow from the existence of a continuously-turning tangent. To show this we first modify the Greek-key curve by replacing the Greek key by the arc shown in Diagram 10. This consists of three arcs, each of which is a quarter-cycle of a sine-curve. Reduced and compressed copies are fitted together as before, and the resulting arc has a continuous tangent everywhere, even at the origin. Clearly it does not have the arc/chord property there. Secondly we modify this curve as follows. S_0 is still as in Diagram 10, but for S_1 the number of small quarter-cycles is doubled, as in Diagram 11 (for clarity we



DIAG. 10



DIAG. 11

have not compressed it yet). This number is doubled again for S_2 and so on. S is now not rectifiable, although the tangent still turns continuously.

References

1. The thirteen books of Euclid's elements, trans. by Sir Thomas L. Heath, Cambridge, 1926.
2. The works of Archimedes, ed. by T. L. Heath, Cambridge, 1897. (on spirals.)
3. Observations sur la composition des mouvements, Roberval, Mémoires de l'Académie Royale des Sciences, 6 (1730).
4. G. T. Whyburn, What is a curve?, Amer. Math. Monthly, 49 (1942) 493–497.
5. H. A. Thurston, On the definition of a tangent-line, Amer. Math. Monthly, 71 (1964).
6. G. H. Hardy, A Course of Pure Mathematics, Cambridge University Press, 1908.
7. A. J. Ward, On Jordan curves possessing a tangent everywhere, Fund. Math., 28 (1937) 280–288.
8. G. Valiron, Sur les courbes qui admettent une tangente en chaque point, Ann. of Math., 2 (1927) 46–51.
9. T. M. Flett, The definition of a tangent to a curve, Edinburgh Math. Notes, 41 (1957) 1–9.

ANSWERS

A444. Let $T_1 \cdots T_n$ be the lineup (T_1 is the first place team). T_2 could have lost only against T_1, since T_1 won all games and T_2 needs one loss. T_3 obviously lost against T_1 (the all out winner) and against T_2, which needs only one loss and already has one. Continuing this reasoning to T_n proves the theorem in the affirmative.

A445. $6k(2k-1)+1=y^3$ implies that $8k^3=y^3+(2k-1)^3$. This is possible only if $k=1/2$ or zero which contradicts the hypothesis.

A446. In a system of numeration with base r, the sum of the distinct digits $0+1+2+\cdots+(r-1)$ is $r(r-1)/2$, a triangular number. If the base is odd, $r(r-1)/2$ is an integer so the sum is a multiple of r. If the base is even, the sum is $(\overline{r-1}+0)/2$. Since $r-1$ is odd the units digit of the sum is 10/2 or one-half the base of numeration.

A447. The equation may be written as $2/3+(2/3)^2=6/9+4/9=10/9$ or or $1.1111\cdots$

A448. We have $a_n=r_n-r_{n+1}$. Also $f(r_n)\leqq f(x)$ for all x in $[r_{n+1}, r_n]$. It follows that

$$a_nf(r_n) \leqq \int_{r_{n+1}}^{r_n} f(x)dx.$$

That is

$$\sum_{n=1}^{N} a_nf(r_n) \leqq \int_{r_{N+1}}^{r_1} f(x)dx \int_0^A f(x)dx$$

for $r_{N+1}>0$.

Noting that $a_nf(r_n)>0$, the result follows.

(Quickies on page 52.)

THE DISTRIBUTION OF QUADRATIC RESIDUES IN FIELDS OF ORDER P^2

N. R. HARDMAN and J. H. JORDAN, Washington State University

1. Introduction. In this paper small Latin letters will represent integers and small Greek letters will represent Gaussian integers, $a+bi$.

Let p be a prime of the form $4k+3$ and let $\hat{p}=\{a+bi: |a|, |b|<p/2\}$. It was established in [1] and [2] that $\hat{p}$ is a complete residue system modulo p in the Gaussian integers. This combined with the fact that p is a Gaussian prime implies that $\hat{p}$ is *a representation of a finite field with p^2 elements.*

Let $\alpha\neq 0$ be an element of $\hat{p}$. If $\eta^2\equiv\alpha \pmod p$ is solvable, then α is said to be a quadratic residue modulo p. If α is not a quadratic residue modulo p then it is a quadratic nonresidue modulo p. The quadratic residues for 3, 7, 19, and 31 are plotted in Figures 1, 2, 3 and 4 respectively.

Recall that the Legendre symbol, (a/q), $a\not\equiv 0 \pmod q$, for q an odd real prime is defined to be 1 if a is a quadratic residue modulo q and -1 if a is a quadratic nonresidue modulo q. Analogously, the symbol $\langle\alpha/p\rangle$, $\alpha\not\equiv 0 \pmod p$, will be defined to be 1 or -1 depending on whether α is a quadratic residue modulo p or not. The symbol $\langle\alpha/p\rangle$ has some of the pleasant properties of the usual Legendre symbol namely $\langle\alpha/p\rangle\langle\beta/p\rangle=\langle\alpha\beta/p\rangle$, and if $\alpha\equiv\beta \pmod p$, then $\langle\alpha/p\rangle=\langle\beta/p\rangle$.

By examining Figures 1–4 many obvious observations can suggest questions like:

1. Are the axes always quadratic residues?
2. Under what conditions will the diagonals be quadratic residues?
3. Are the quadratic residues always symmetric with respect to x axis? y axis? origin? and diagonals?

It is the purpose of this paper to answer these three queries and some other not so obvious questions about the patterns of quadratic residues and to establish links between the symbols $\langle/\rangle$ and $(/)$ and a link between primitive roots.

2. Euler's criteria. The generalization of Euler's criteria would be

THEOREM 1. *If $p\nmid\alpha$ then $\langle a/p\rangle\equiv\alpha^{(p^2-1)/2} \pmod p$.*

Proof. Since $\hat{p}$ is a finite field there is a generator, γ ,which generates the nonzero elements of $\hat{p}$. This γ would be called a primitive root modulo the Gaussian prime p. If there is a β such that $\beta^2\equiv\alpha \pmod p$ and $\gamma^s\equiv\beta \pmod p$, then $\gamma^{2s}\equiv\alpha \pmod p$; hence $\gamma^{2s(p^2-1)/2}\equiv\alpha^{(p^2-1)/2} \pmod p$. But $(\gamma^{p^2-1})^s\equiv 1 \pmod p$ and so $\langle\alpha/p\rangle\equiv\alpha^{(p^2-1)/2} \pmod p$. If $\langle\alpha/p\rangle=-1$, then $\gamma^{2t+1}\equiv\alpha \pmod p$ and $\gamma^{(2t+1)(p^2-1)/2}\equiv\alpha^{(p^2-1)/2} \pmod p$. But $\gamma^{(p^2-1)t}\equiv 1 \pmod p$ and $\gamma^{(p^2-1)/2}\equiv -1 \pmod p$ by the properties of a generator. Hence $-1=\langle\alpha/p\rangle\equiv\alpha^{(p^2-1)/2} \pmod p$ and the criterion is established.

To answer question 1 we have

COROLLARY 1. $\langle a/p\rangle=\langle ai/p\rangle=1$.

Proof. By Fermat's little theorem, $a^{p-1}\equiv 1 \pmod p$; hence $a^{(p-1)(p+1)/2}\equiv 1 \pmod p$ and so $\langle a/p\rangle=1$. Since $(p^2-1)/2=4k$ and $\langle i/p\rangle\equiv(i^4)^k\equiv 1 \pmod p$, it follows that $\langle i/p\rangle=1$; hence $\langle ai/p\rangle=1$.

Quadratic Residues Modulo 3

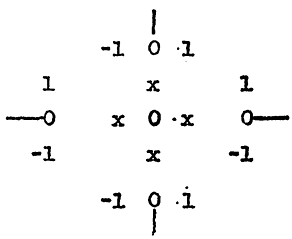


FIG. 1

Quadratic Residues Modulo 7

Union Jack

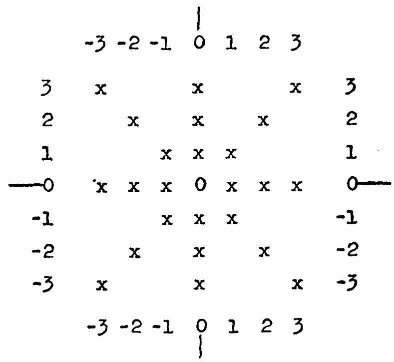


FIG. 2

Quadratic Residues Modulo 19

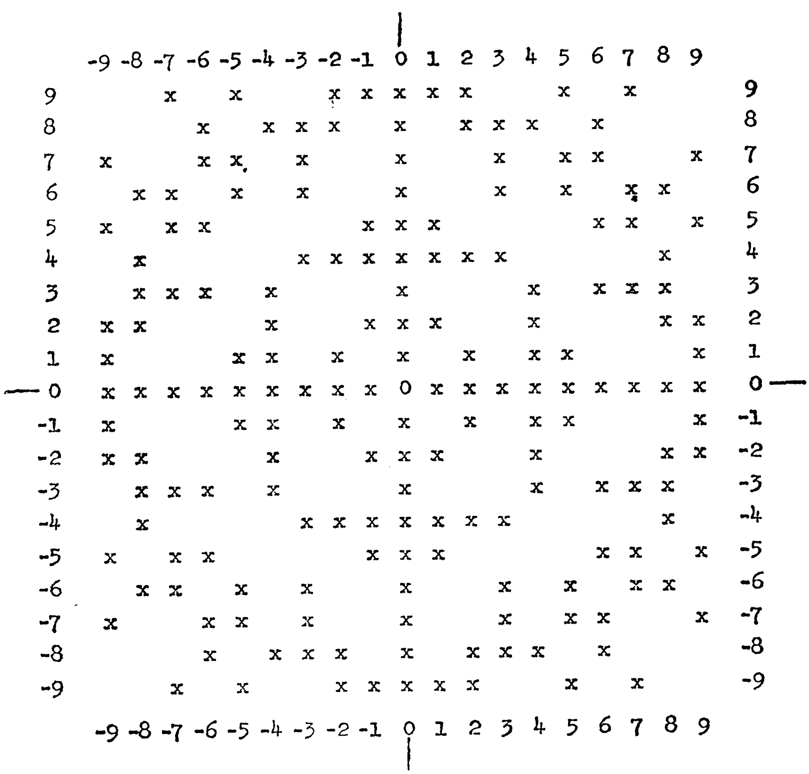


FIG. 3

Quadratic Residues modulo 31

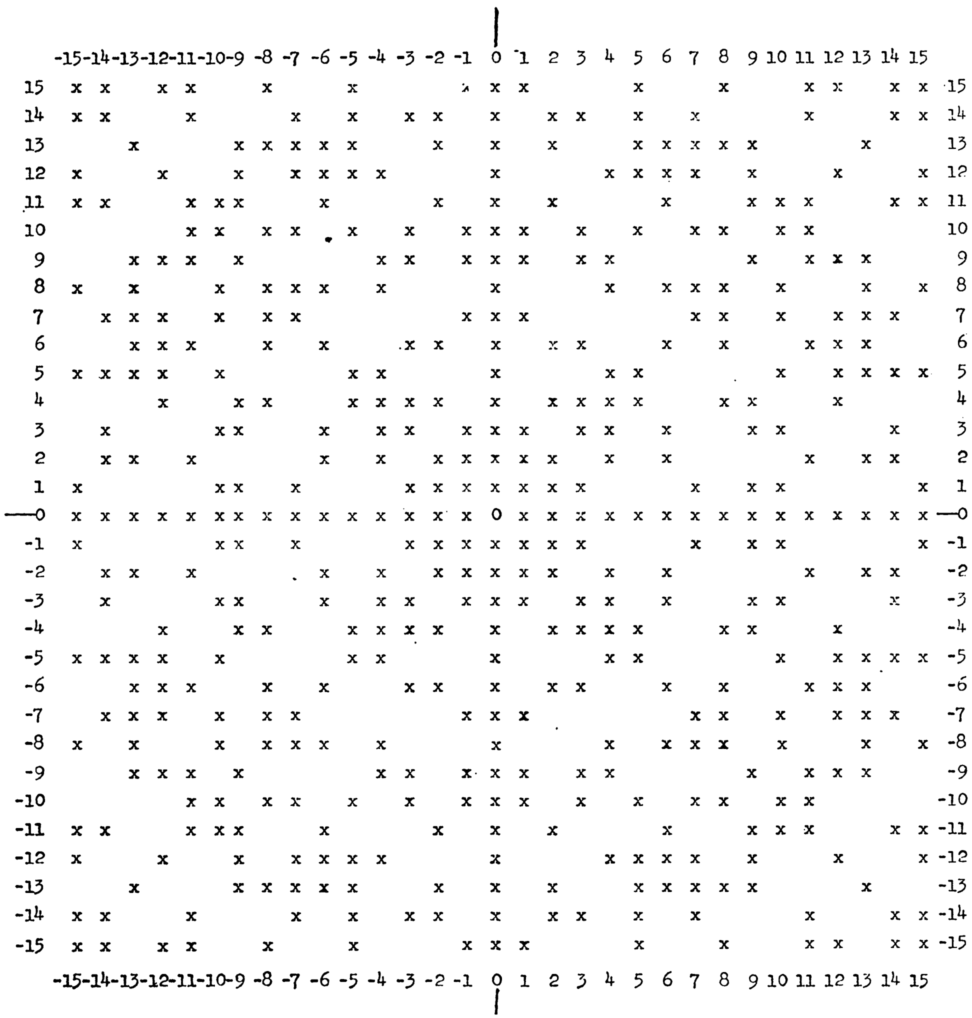


FIG. 4

COROLLARY 2. $\langle a+bi/p\rangle=\langle -b+ai/p\rangle=\langle -a-bi/p\rangle=\langle b-ai/p\rangle$.

Clearly each symbol is equal to $i^s(a+bi)$, $s=0, 1, 2, 3$ and, by Corollary 1, $\langle i^s/p\rangle=1$.

To answer question 2 we have

COROLLARY 3. $\langle a+ai/p\rangle=\langle a-ai/p\rangle=(-1)^{(p+1)/4}$.

Proof. To show $\langle a+ai/p\rangle=(-1)^{(p+1)/4}$ it suffices to establish that $\langle 1+i/p\rangle=(-1)^{(p+1)/4}$ since $\langle a/p\rangle=1$. By Euler's criteria

$$\langle 1+i/p\rangle \equiv (1+i)^{(p^2-1)/2}$$

$$\equiv (2i)^{(p^2-1)/4}$$
$$\equiv 2^{(p^2-1)/4} i^{(p^2-1)/4} \pmod{p}.$$

But $(p+1)/4$ is an integer so $(2^{p-1})^{(p+1)/4} \equiv 1 \pmod{p}$ and $i^{(p^2-1)/4} = (-1)^{(p^2-1)/8} = (-1)^{(p+1)/4}$. Hence $\langle a+ai/p\rangle = (-1)^{(p+1)/4}$. Notice that since $\langle -i/p\rangle = 1$ it follows that $\langle a+ai/p\rangle = \langle -i/p\rangle\langle a+ai/p\rangle = \langle a-ai/p\rangle$.

3. Symmetry. The answer to question 3 uses

THEOREM 2. $\langle a+bi/p\rangle = \langle a-bi/p\rangle$.

Proof. If $(c+di)^2 \equiv a+bi \pmod{p}$, then $(c-di)^2 \equiv a-bi \pmod{p}$. Hence $\langle a+bi/p\rangle = \langle a-bi/p\rangle$.

This gives symmetry with respect to the x axis. Since $\langle -1/p\rangle = 1$ it follows that $\langle a+bi/p\rangle = \langle -a+bi/p\rangle$ so the quadratic residues are symmetric with respect to the y axis and the origin. Since $\langle i/p\rangle = 1$ it follows that $\langle a+bi/p\rangle = \langle b+ai/p\rangle$ so the quadratic residues are symmetric with respect to the diagonals.

4. The number of residues per line. On each line other than the axes there is exactly one more nonresidue than there are residues. Due to the symmetry with respect to the x and y axes the distribution can be stated more precisely by

THEOREM 3. *If $b \neq 0$ and $c \neq 0$, then*

$$\sum_{a=1}^{(p-1)/2} \langle a + bi/p\rangle = \sum_{d=1}^{(p-1)/2} \langle c + di/p\rangle = -1.$$

Proof. There are $p^2-1/2$ quadratic residues and $2p-2$ of them reside on axes. There are therefore $(p^2-1)/2-2p+2$ residues equally distributed in the four quadrants, a total of $(p^2-4p+3)/8$ residues in each quadrant. The $(p^2-1)/2$ nonresidues are also equally distributed in the four quadrants for a total of $(p^2-1)/8$ nonresidues in each quadrant. Hence

$$\sum_{b=1}^{(p-1)/2} \sum_{a=1}^{(p-1)/2} \langle a + bi/p\rangle = (p^2 - 4p + 3)/8 - (p^2 - 1)/8 = (1 - p)/2.$$

Since $b \neq 0$ there is an x_b such that $bx_b \equiv 1 \pmod{p}$. Since $\langle x_b/p\rangle = 1$ it follows that

$$\sum_{a=1}^{(p-1)/2} \langle a + bi/p\rangle = \sum_{a=1}^{(p-1)/2} \langle ax_b + i/p\rangle.$$

Now, as can be recalled from the proof of Gauss' Lemma,

$$\{x_b, 2x_b, \cdots, (p-1)/2x_b\}$$

are in some way congruent to

$$\{\epsilon_1 1, \epsilon_2 2, \epsilon_3 3, \cdots, \epsilon_{(p-1)/2}(p-1)/2\} \text{ modulo } p, \quad \text{where} \quad \epsilon_j = \pm 1.$$

But because of the symmetry with respect to the y axis established by Theorem 2, i.e., $\langle a+bi/p\rangle = \langle -a+bi/p\rangle$, the following equality holds:

$$\sum_{a=1}^{(p-1)/2} \langle a+bi/p\rangle = \sum_{a=1}^{(p-1)/2} \langle ax_b+i/p\rangle = \sum_{j=1}^{(p-1)/2} \langle \epsilon_j j+i/p\rangle = \sum_{a=1}^{(p-1)/2} \langle a+i/p\rangle.$$

Summing this expression over $1\leqq b\leqq (p-1)/2$, it follows that

$$-(p-1)/2 = \sum_{b=1}^{(p-1)/2}\sum_{a=1}^{(p-1)/2} \langle a+bi/p\rangle = (p-1)/2\sum_{a=1}^{(p-1)/2} \langle a+i/p\rangle;$$

hence

$$\sum_{a=1}^{(p-1)/2} \langle a+i/p\rangle = -1 = \sum_{a=1}^{(p-1)/2} \langle a+bi/p\rangle.$$

A similar argument settles the case where

$$\sum_{d=1}^{(p-1)/2} \langle c+di/p\rangle = -1.$$

5. A connection between $\langle/\rangle$ and $(/)$. The following interesting result exists.

THEOREM 4. $\langle a+bi/p\rangle = (a^2+b^2/p)$.

Proof. If $\langle a+bi/p\rangle = 1$, then there is a $c+di$ such that $(c+di)^2\equiv a+bi$ (mod p) and consequently $(c-di)^2\equiv a-bi$ (mod p). Hence $(c^2+d^2)^2\equiv a^2+b^2$ (mod p) or $(a^2+b^2/p)=1$.

On the other hand, if $\langle a+bi/p\rangle = -1$, consider the arithmetic progression $\{4pn+2p-1\}$. Since $4p$ and $2p-1$ are relatively prime, there is a prime q in the progression. Since $p=4k+3$, $q=4(pn+2k+1)+1$ and hence q is representable as $q=c^2+d^2$. But $q\equiv -1$ (mod p) and so $(q/p)=(c^2+d^2/p)=-1$. By the first part of this proof this implies that $\langle c+di/p\rangle=-1$. Therefore $\langle a+bi/p\rangle\langle c+di/p\rangle$ $=\langle ac-bd+(ad+bc)i/p\rangle=1$. Again using the first part of the proof, this implies $((ac-bd)^2+(ad+bc)^2/p)=1$. But $(ac-bd)^2+(ad+bc)^2=(a^2+b^2)(c^2+d^2)$ and so $(a^2+b^2/p)(c^2+d^2/p)=1$; hence $(a^2+b^2/p)=-1$ and so $\langle a+bi/p\rangle=(a^2+b^2/p)$. An interesting consequence of Theorems 3 and 4 is

COROLLARY. *If $b\neq 0$, then* $\sum_{a=1}^{(p-1)/2}(a^2+b^2/p)=-1$.

Proof. $-1=\sum_{a=1}^{(p-1)/2}\langle a+bi/p\rangle=\sum_{p=1}^{(p-1)/2}(a^2+b^2/p)$.

6. A connection between primitive roots. Let γ be a primitive root modulo the Gaussian prime p.

LEMMA 1. *If $\gamma^s\equiv a$ (mod p), then $s\equiv 0$ (mod $p+1$).*

Proof. Since $\gamma^s\equiv a$ (mod p), then $\gamma^{s(p-1)}\equiv a^{p-1}\equiv 1$ (mod p); therefore $p^2-1\mid s(p-1)$ or $p+1\mid s$.

THEOREM. *If g is a primitive root modulo p and $\gamma^s\equiv g$* (mod p), *then $s=(p+1)h$ where $(h, p-1)=1$.*

Proof. By hypothesis $\gamma^s\equiv\gamma^{h(p+1)}\equiv g$ (mod p). Raise both sides to the $(p-1)/$

$(p-1,\ h)$ power yielding $g^{(p-1)/(p-1,h)} \equiv (\gamma^{p^2-1})^{h/(p-1,h)} \equiv 1 \pmod{p}$; hence $p-1 \mid (p-1)/(p-1,\ h)$ or $(p-1,\ h)=1$.

COROLLARY. *γ^{p+1} is a primitive root modulo p.*

Research for this paper was supported in part by NSF Grant No. G22765/0009 (Undergraduate research), NSF Grant No. GP-6227 and WSU Grant in aids for research project No. 728.

References

1. N. R. Hardman and J. H. Jordan, A minimal problem connected with complete residue systems in the Gaussian integers, Amer. Math. Monthly, 74, 5 (1967) 559–561,

2. J. H. Jordan and C. J. Potratz, Complete residue systems in the Gaussian integers, this MAGAZINE, 38 (1965) 1–12.

THE BUTTERFLY PROBLEM—EXTENSIONS, GENERALIZATIONS

WILLIAM I. JACOBSON, Sheepshead Bay High School, Brooklyn

In its usual form the Butterfly Problem might be stated: through M, the midpoint of chord AB of a circle, two other chords, CD and EF, are drawn. Also ED and CF are drawn intersecting AB in P and Q respectively. Then $PM=MQ$ (Figure 1). In [1] Klamkin shows that the chords CD and EF need not pass through M. But if, instead, they intersect AB in S and R respectively so that $RM=MS$, then again $PM=MQ$ (Figure 2).

A generalization of this latter result can be obtained by considering the circle to be a special case of a conic and the two pairs of lines CD, EF and ED, CF also to be special cases of conics (degenerate). A theorem will first be given in reference to Figure 2, generalized.

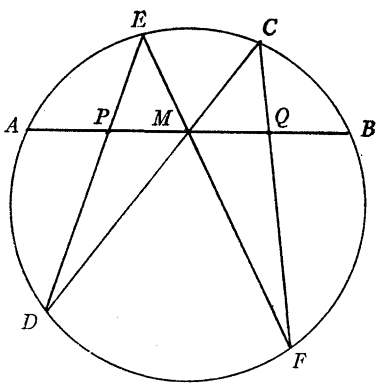


FIG. 1

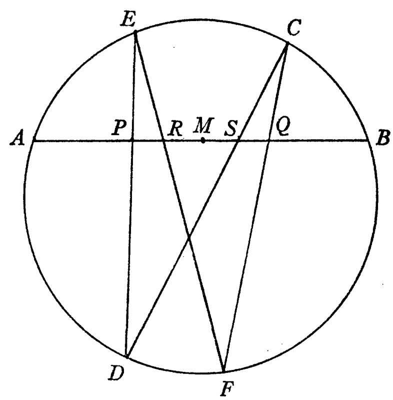


FIG. 2

THEOREM I. *Three conics pass through the same four distinct points E, C, F, and D, no three of which are collinear. On a common secant, these conics intercept chords AB, RS, and PQ. Then if M is the midpoint of AB and of RS, M is also the midpoint of PQ. (E and D do not have to be on opposite sides of AB.)*

The proof of this theorem will be based on two lemmas.

LEMMA 1. (Figure 3). *Let the x-axis be along chord AB of a conic. Select as the origin a point M which is not on the conic and is between A and B. If the conic is represented by*

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

then M is the midpoint of AB if and only if the x term is missing ($d = 0$).

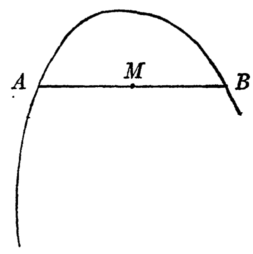


FIG. 3

Proof. The conic intersects the x-axis in A and B, origin at M. If, in the general conic, we let $y = 0$, we get $ax^2 + dx + f = 0$, whose roots we may call h and k. A and B are distinct so that $a \neq 0$.

(a) If M is the midpoint of AB, then $h + k = 0$ and $-(d/a) = 0$; $a \neq 0$ and therefore $d = 0$.

(b) Conversely, if $d = 0$, then $-(d/a) = 0$ so that $h + k = 0$. Therefore M is the midpoint of AB.

LEMMA 2. *If three distinct conics pass through the same four distinct points, no three of which are collinear, then each conic is a linear combination of the other two.*

Proof. The three conics $f_1 = 0$, $f_2 = 0$, and $f_3 = 0$ are distinct and pass through four distinct points (x_1, y_1), (x_2, y_2), (x_3, y_3), and (x_4, y_4). Since five points, no four of which are collinear, determine a conic, there is a point (x_5, y_5) which is on $f_3 = 0$, but not on either $f_1 = 0$ or $f_2 = 0$, so that $f_1(x_5, y_5) \neq 0$ and $f_2(x_5, y_5) \neq 0$, but $f_3(x_5, y_5) = 0$.

Let

$$g(x, y) \equiv f_1(x, y) - \frac{f_1(x_5, y_5)}{f_2(x_5, y_5)} f_2(x, y).$$

By inspection $g = 0$ and $f_3 = 0$ pass through the same five points and therefore represent the same conic section. (Note: $g = 0$ is not linear since it passes through noncollinear points; nor is g identically zero, for then $f_1 = kf_2$, and $f_1 = 0$ and $f_2 = 0$ would not be distinct, contrary to hypothesis.)

Hence

$$f_3 = k_1 g = k_1 f_1 + k_2 f_2, \qquad (k \neq 0,\ k_1 \neq 0,\ k_2 \neq 0).$$

Using these two lemmas we may conclude as follows: (Figure 2 with x-axis chosen along AB): Since M is the midpoint of AB and of RS, the x term will be missing in each conic. And since the third conic is a linear combination of the other two, the x term will likewise be missing in the third conic. Hence M is also the midpoint of PQ.

This theorem can be stated in a somewhat different form:

Consider a family of conics through the same four distinct points, no three of which are collinear. If any one pair of these conics intercepts between them two equal segments on a given secant, then so will any other pair of conics in the family.

(One conic intersects the secant in an outer pair of points, and the other in an inner pair. See Figure 4.)

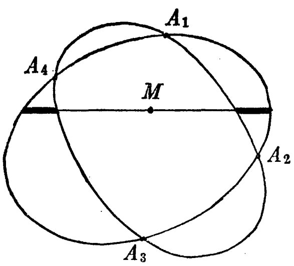


FIG. 4

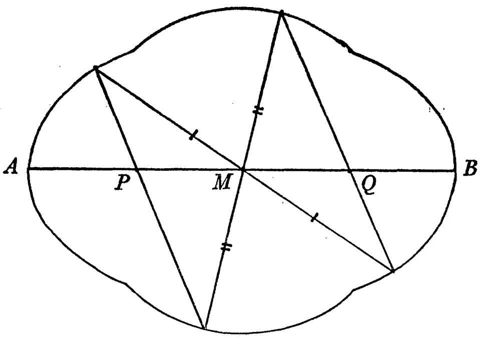


FIG. 5

It might be pointed out that there are butterfly situations other than those covered in Theorem I. This can be seen in the somewhat trivial illustration in Figure 5. This figure is a composite of two arcs of a circle and two arcs of an ellipse. M is the center of the major axis AB of the ellipse, and is also the center of the arcs of the circle. $PM = MQ$ by simple congruence, and this holds for any two chords, distinct from AB, through M. Obviously this composite figure is not a conic section.

Generally, then, when may the butterfly property arise? To help answer this question, it can be shown that there is a quantitative aspect which is characteristic of the butterfly property.

THEOREM II. (Figure 6). *The sum of the reciprocals of the ordinates of P_1 and P_3 is the same as for P_2* and *P_4 if and only if M is the midpoint of AB. (M is the*

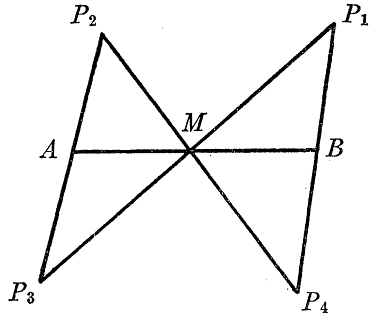


FIG. 6

origin, with the x-axis along AB. P_1P_3 and P_2P_4 are straight lines. P_1P_4 and P_2P_3 are a pair of straight lines or another conic. P_2 and P_3 do not have to be on opposite sides of AB).

Proof. Consider the general form, $ax^2+bxy+cy^2+dx+ey+f=0$, of a conic $P_3P_2P_1P_4$. M is not on the conic; A and B are distinct as in Lemma 1, so that $a\neq 0$, $f\neq 0$. Let the equation of P_1P_3 be $x=my$. Substituting my for x in the general form gives $y^2(am^2+bm+c)+y(dm+e)+f=0$. The ratio r_{13}, of the sum of the roots to the product, of this equation is

$$\frac{y_1+y_3}{y_1y_3}=-\frac{dm+e}{f}=r_{13}.$$

(The coefficient of y^2 is not zero, since P_1 and P_3 are distinct. Also $y_1\neq 0$, $y_3\neq 0$, $f\neq 0$.) Similarly, letting the equation of P_2P_4 be $x=ny$, we get

$$\frac{y_2+y_4}{y_2y_4}=-\frac{dn+e}{f}=r_{24}\ (y_2\neq 0,\ y_4\neq 0, f\neq 0).$$

Since P_1P_3 and P_2P_4 are distinct lines, $m\neq n$. Hence $r_{13}=r_{24}$ if and only if $d=0$, or from Lemma 1, if and only if M is the midpoint of AB. (Note: when M is the midpoint of AB, each of the above ratios equals $-(e/f)$. For a particular conic this is constant and is independent of either m or n when the axis is along AB.)

In the above discussion the point M was not on the conic. For completeness it might be mentioned that when M is on the conic through $P_1P_2P_3P_4$, the conic is a degenerate case (lines P_1P_3 and P_2P_4) and the distances $AM=MB=0$, so that M might be considered the midpoint of a zero AB.

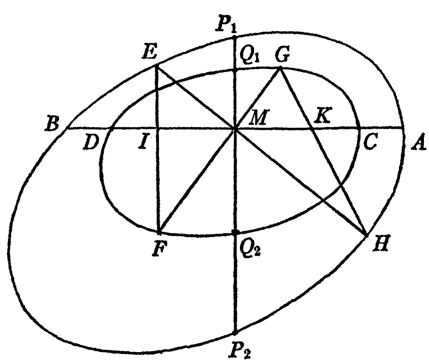


FIG. 7

This property of the ordinates can be used to create butterfly situations, such as using a chord from one conic and a second chord from another conic. To illustrate: select two points on the y-axis (Figure 7), such as $P_1(0, 3)$ and $P_2(0, -6)$. Also select a third point such as $Q_1(0, 2)$. Now find a $Q_2(0, k)$ such that

$$\frac{1}{3}+\frac{1}{-6}=\frac{1}{2}+\frac{1}{k}.$$

Solving, $k=-3$.

On the x-axis select two points $A(r, 0)$ and $B(-r, 0)$. Draw one conic through P_1, P_2, A, and B. Also select two points $C(s, 0)$ and $D(-s, 0)$, and draw one of the conics through Q_1, Q_2, C, and D. Also draw GMF, a chord of one conic and EMH a chord of the other. Draw EF and GH intersecting the x-axis in I and K respectively. Noting that the sum of the reciprocals of ordinates is the same for G, F as for Q_1, Q_2, which is the same as for P_1, P_2, and which is the same as for E, H, we can conclude that E, F, G, and H form a set of butterfly points with respect to M and the x-axis. Hence $IM=MK$.

Reference

1. M. S. Klamkin, An extension of the butterfly problem, this MAGAZINE, 38 (1965) 206–208.

ON THE BUTTERFLY PROPERTY

G. D. CHAKERIAN, G. T. SALLEE, University of California at Davis,
M. S. KLAMKIN, Ford Scientific Laboratory, Dearborn, Michigan

It is an old result [3] that the "butterfly" property holds for circles, i.e., if C is the midpoint of an arbitrary chord AB, and if DE and FG are any two chords through C, then $\overline{CH}=\overline{CI}$ and $\overline{CJ}=\overline{CK}$. (See Figure 1.)

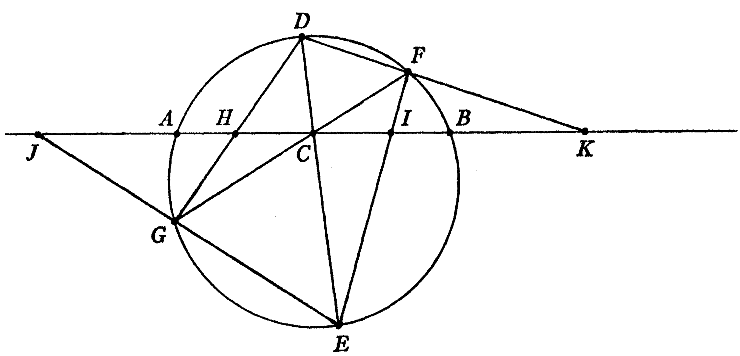


FIG. 1

The nomenclature for the problem comes from the resemblance of the figure $DGCFEC$ to a butterfly. It is also known that the butterfly property holds for ellipses. This follows immediately from the result for circles by parallel projection, which transforms midpoints into midpoints.

In a paper [2] by one of the authors on an extension of the Butterfly Problem, it was conjectured that the butterfly property characterizes ellipses. We now establish this result for ovals, i.e.,

THEOREM. *Let S be a closed, bounded, plane convex set with the following property: whenever C is the midpoint of a chord AB, and DE and FG are any two chords containing C, then $\overline{CH}=\overline{CI}$ (as in Figure 1). Then S is an ellipse.*

Proof. It will be convenient to first establish that S is centrosymmetric.

There exists a pair of chords, GH and CD, bisecting each other in a point O. (There are a number of ways to see this. For example, it is well known that S admits an inscribed square, and the diagonals of this square provide the required chords. More directly, for each direction θ, let $M(\theta)$ be the set of midpoints of all chords in the direction θ. It is not difficult to show that the $M(\theta)$ are continuous curves, and that any two of these curves intersect in an interior point of S. Such an intersection provides us with a pair of chords bisecting each other. Hence one has that the chords GH and CD can even be chosen to have any prescribed directions.) Now let AB be any chord containing O (Figure 2). The butterfly property implies $\overline{OE}=\overline{OF}$. It follows that AD is parallel to CB; hence $\overline{OA}=\overline{OB}$.

Next, observe that the butterfly property implies the following property, which we shall refer to in the sequel as the "weak butterfly property": if C is the midpoint of a chord AB, and if DE and FG are chords through C, then DF is parallel to AB if and only if GE is parallel to AB (with the notation as in Figure 1). In fact, even restricting attention to the quadrilateral $DGEF$ in Figure 1, one may see that if $\overline{CH}=\overline{CI}$, then DF is parallel to HI if and only if GE is parallel to HI.

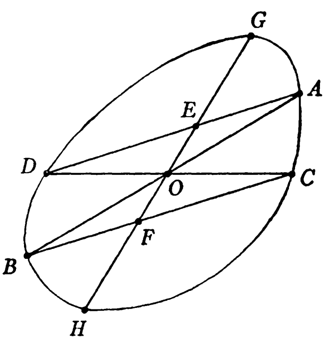


FIG. 2

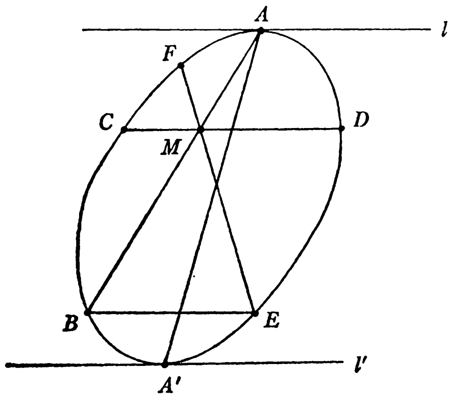


FIG. 3

We now prove that the midpoints of any set of parallel chords of S lie on a straight line.

Let l and l' be parallel supporting lines of S. By the centro-symmetry of S, they will either each contain a single point of the boundary, or they will have equal and parallel segments in common with the boundary. We shall consider these two cases separately.

Suppose l and l' intersect the boundary of S in points A and A' respectively (Figure 3).

Suppose that the midpoint M of some chord CD parallel to l does *not* lie on AA'. Then let B be such that the chord AB contains M, and E such that BE is a chord parallel to CD. Finally, let F be such that EF is a chord containing M. The weak butterfly property implies that FA should be parallel to BE, which is impossible since F cannot lie on l. Thus the midpoints of all chords parallel to l lie on the line AA'.

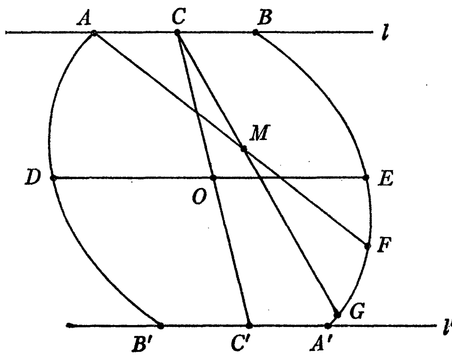


FIG. 4

Now suppose l intersects the boundary of S in a segment AB and l' intersects the boundary in the equal and parallel segment $A'B'$ (Figure 4). Let C and C' be the midpoints of AB and $A'B'$ respectively, and let DE be the chord parallel to AB and containing the center O of S. Suppose that the midpoint M of some chord parallel to AB does not lie on CC'. We may suppose without loss of generality that M lies in the open region $COEB$, as indicated in Figure 4. Then the ray AM intersects the boundary of S in a point F not on l'. Let G be such that the chord CG contains M. Note that G is on the arc $C'A'F$. The weak butterfly property implies that AC is parallel to GF, which is clearly impossible. Thus the midpoints of all chords parallel to l (and not contained in l and l') lie on line CC'.

This completes the proof that the midpoints of any set of parallel chords of S lie on a straight line. But it is well known that this property characterizes ellipses (see [1], p. 92); hence S is an ellipse. This completes the proof of the theorem.

Remark. The following characterization of ellipses is not difficult to prove: if S is a closed and bounded plane convex set such that for a dense set of directions the midpoints of parallel chords lie on a straight line, then S is an ellipse. Hence, in the above proof, one does not really need to consider the case where l intersects the boundary of S in a segment since the directions for which l intersects the boundary in a single point comprise a dense set.

We are indebted to Dr. Leon Bankoff who supplied the early references below from his unpublished manuscript on the history of the Butterfly Problem.

References

1. H. Busemann, The Geometry of Geodesics, Academic Press, New York, 1955.
2. M. S. Klamkin, An extension of the Butterfly Problem, this MAGAZINE, 38 (1965) 206–208
3. The Gentleman's Diary, 1815, pp. 39–40, Question 1029. Miles Bland, Geometrical Problems, Cambridge, 1819, p. 228.

Correction for, "On the Volume of a Class of Truncated Prisms and Some Related Centroid Problems," by M. S. Klamkin: For the four simultaneous nonlinear equations on p. 180 (1968), this MAGAZINE, there is also the symmetric solution $m=s=0$, $n=r=-1$. However, this latter solution is ruled out by the tacit requirement that A, B, C, D be four vertices of a convex quadrilateral in the indicated order.

ON THE PRODUCT OF DIAGONAL ELEMENTS OF A POSITIVE MATRIX

A. R. AMIR-MOÉZ and G. E. JOHNSTON, Texas Technological College

Let A be a positive transformation on an n-dimensional unitary space E_n. Then

$$\det A \leqq \prod_{i=1}^{n} a_{ii}.$$

A proof of this proposition is given in [2]. In this article we use geometric properties of vectors in E_n to prove the theorem; particularly, we discuss the problem in a Euclidean plane in order to explain geometric motives for techniques of the proof.

1. LEMMA. *Let A be a positive transformation on E_n. Then there exists a transformation B such that $BB^* = A$, where B^* is defined by $(B\xi, \eta) = (\xi, B^*\eta)$, for all ξ and η in E_n.*

This is a well known theorem and we omit the proof [3].

2. A geometric interpretation. We shall give a geometric interpretation of Lemma 1 in the Euclidean plane. Let the matrix of A with respect to an orthonormal basis $\{\alpha_1, \alpha_2\}$ be

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Let the matrix of B with respect to the same basis be

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}.$$

Suppose $\xi = b_{11}\alpha_1 + b_{12}\alpha_2$ and $\eta = b_{21}\alpha_1 + b_{22}\alpha_2$. Then

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} (\xi, \xi) & (\xi, \eta) \\ (\eta, \xi) & (\eta, \eta) \end{pmatrix}.$$

One can easily show that $\mathfrak{A}$, the area of the triangle formed by ξ and η, is

$$\mathfrak{A} = \frac{1}{2}\left[\begin{vmatrix} (\xi, \xi) & (\xi, \eta) \\ (\eta, \xi) & (\eta, \eta) \end{vmatrix}\right]^{1/2}.$$

For the proof see [1].

3. THEOREM. *Let A be a positive transformation on the plane whose matrix with respect to an orthonormal basis $\{\alpha_1, \alpha_2\}$ is*

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

Then $\det A \leqq a_{11}a_{22}$.

Proof. Let B be the linear transformation which was described in Section 2. Then the matrix of A will be

$$\begin{pmatrix} (\xi, \xi) & (\xi, \eta) \\ (\eta, \xi) & (\eta, \eta) \end{pmatrix}$$

and

$$\det A = \|\xi\|^2 \cdot \|\eta\|^2 - |(\xi, \eta)|^2 \leqq \|\xi\|^2 \cdot \|\eta\|^2 = a_{11}a_{22}.$$

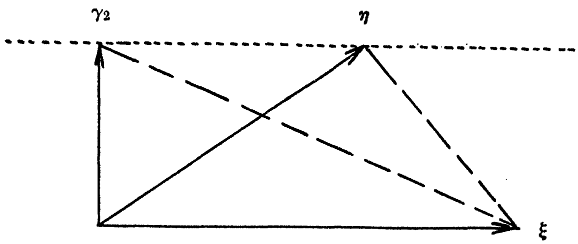


FIG. 1

But it is quite difficult to generalize this proof. Thus we supply a geometric proof. It is clear that $\det A = 4\mathfrak{A}^2$, where $\mathfrak{A}$ is the area described in Section 2. Let $\gamma_1 = \xi$ (Figure 1) and γ_2 be a vector perpendicular to ξ ending on the line through the endpoint of η parallel to ξ. Then the area of the right triangle formed by γ_1 and γ_2 is the same as $\mathfrak{A}$. Thus

$$\det A = \begin{vmatrix} (\gamma_1, \gamma_1) & 0 \\ 0 & (\gamma_2, \gamma_2) \end{vmatrix} = (\gamma_1, \gamma_1)(\gamma_2, \gamma_2).$$

We observe that

$$\gamma_1 = \xi \quad \text{and} \quad \gamma_2 = \eta - \left(\eta, \frac{\xi}{\|\xi\|}\right)\frac{\xi}{\|\xi\|} = \eta - \frac{1}{\|\xi\|^2}(\eta, \xi)\xi.$$

Thus

$$(\gamma_1, \gamma_1) = (\xi, \xi) \quad \text{and} \quad (\gamma_2, \gamma_2) = (\eta, \eta) - \frac{|(\eta, \xi)|^2}{\|\xi\|^2} \leqq (\eta, \eta).$$

Therefore $\det A = (\gamma_1, \gamma_1)(\gamma_2, \gamma_2) \leqq (\xi, \xi)(\eta, \eta) = a_{11}a_{22}$.

Now we shall use the ideas of this proof for the general case in the following theorem.

4. THEOREM. *Let A be a positive transformation on E_n. Suppose the matrix of A with respect to an orthonormal basis χ is (a_{ij}). Then*

$$\det A \leqq \prod_{i=1}^{n} a_{ii}.$$

Proof. By Lemma 1 there exists a linear transformation B on E_n such that $BB^*=A$. Let the matrix of B with respect to χ be (b_{ij}). Then the matrix of B^* with respect to χ is $(\bar{b}_{ji})$. Suppose $\xi_i=(b_{i1}, \cdots, b_{in})$. Then $a_{ij}=(\xi_i, \xi_j)$. Now we will use the geometric idea discussed in Section 3. Let $\gamma_1=\xi_1$ and

$$\gamma_k = \xi_k - \sum_{i=1}^{k-1} s_{ki}\gamma_i, \qquad (\gamma_p, \gamma_q) = 0 \quad \text{for } p \neq q,\ 2 \leqq k \leqq n.$$

We note that

$$\begin{aligned} 0 = (\gamma_k, \gamma_i) &= (\xi_k - s_{k1}\gamma_1 - \cdots - s_{k(k-1)}\gamma_{k-1}, \gamma_i) \\ &= (\xi_k, \gamma_i) - s_{ki}(\gamma_i, \gamma_i), \qquad i = 1, \cdots, k-1. \end{aligned}$$

Since $BB^*>0$ it follows that $\xi_i\neq 0$ and thus $\gamma_i\neq 0$ for $i=1, \cdots, n$. Therefore

$$s_{ki} = \frac{(\xi_k, \gamma_i)}{(\gamma_i, \gamma_i)}. \tag{1}$$

Further we observe that

$$\begin{aligned} (\gamma_k, \gamma_k) &= \left(\xi_k - \sum_{i=1}^{k-1} s_{ki}\gamma_i,\ \xi_k - \sum_{i=1}^{k-1} s_{ki}\gamma_i\right) \\ &= (\xi_k, \xi_k) - \sum_{i=1}^{k-1} \left[\bar{s}_{ki}(\xi_k, \gamma_i) + s_{ki}\overline{(\xi_k, \gamma_i)}\right] + \sum_{i=1}^{k-1} | s_{ki} |^2 (\gamma_i, \gamma_i). \end{aligned}$$

Considering (1) we get

$$(\gamma_k, \gamma_k) = (\xi_k, \xi_k) - \sum_{i=1}^{k-1} \frac{| (\xi_k, \gamma_i) |^2}{(\gamma_i, \gamma_i)}.$$

This implies that

$$(\gamma_k, \gamma_k) \leqq (\xi_k, \xi_k). \tag{2}$$

Now let $\gamma_i=(c_{i1}, \cdots, c_{in})$ with respect to χ and let C be the linear transformation whose matrix with respect to χ is (c_{ij}). Then we have $\det A = \det BB^* = \det CC^*$. Since $\{\gamma_1, \cdots, \gamma_n\}$ is a set of nonzero orthogonal vectors, we have $\det CC^* = (\gamma_1, \gamma_1) \cdot \cdots \cdot (\gamma_n, \gamma_n)$. Comparing this with (2) we obtain

$$\det A = \prod_{i=1}^{n} (\gamma_i, \gamma_i) \leqq \prod_{i=1}^{n} (\xi_i, \xi_i) = \prod_{i=1}^{n} a_{ii}.$$

References

1. A. R. Amir-Moéz, Problems of Matrix Techniques, Edwards, Ann Arbor, Michigan, 1965.
2. E. F. Beckenbach and R. E. Bellman, Inequalities, Springer Verlag, 1965.
3. I. N. Herstein, Topics in Algebra, Blaisdell, New York, 1964.

ON WRAPPING OF A CLOSED SURFACE

R. D. GLAUZ, Sacramento, California

Introduction. In the wrapping of fiberglass containers such as solid rocket pressure vessels there is an interesting mathematical problem. The wrapping process consists of wrapping a finite width tape continuously until the container is completely covered. Thus the mathematical problem consists of ensuring a complete coverage with uniform thickness. If we consider Figure 1 we note that the successive wraps occur spaced apart, the distance depending on wrap angle, container length, head design, and other factors based on a structural analysis.

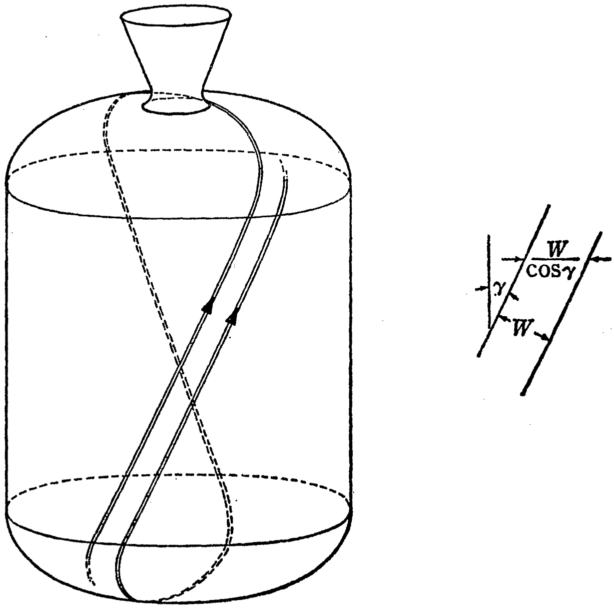


FIG. 1

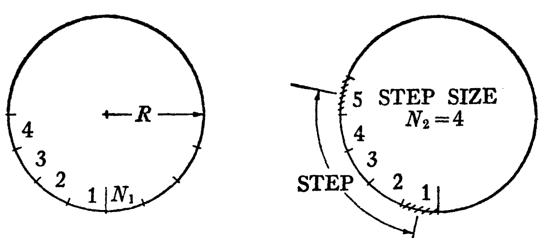


FIG. 2

The circumference of the head can be subdivided into N_1 cells corresponding to possible tape positions as in Figure 2. We have

$$N_1 = \frac{2\pi R}{w/\cos\gamma}.$$

Let the step size be N_2 = number of cells to next successive wrap. Let M be the number of tapes being wrapped simultaneously. The requirements will be established with regard to N_1, N_2, M. The designer has some control in varying these quantities so that these requirements are met.

DEFINITION. *A cycle is a sequence of steps until the initial position is repeated. Cycle length is the number of distinct cells occupied by a cycle.*

THEOREM. *Cycle length* $=(N_1/(N_1, N_2))=\overline{N}_1$ *where* (N_1, N_2) = *greatest common factor of* N_1, N_2.

Proof. (a) Cycle length is not greater than $(N_1/(N_1, N_2))=\overline{N}_1$ since if $N_1=\overline{N}_1\cdot(N_1, N_2)$ and $N_2=\overline{N}_2\cdot(N_1, N_2)$, then $(\overline{N}_1+1)N_2=(\overline{N}_1+1)[\overline{N}_2(N_1, N_2)]$ $=\overline{N}_1\cdot\overline{N}_2\cdot(N_1, N_2)+\overline{N}_2(N_1, N_2)\equiv\overline{N}_2\cdot(N_1, N_2)$ Mod N_1 and $1(N_2)\equiv\overline{N}_2(N_1, N_2)$ Mod N_1. Hence a cycle repeats with period $\overline{N}_1$.

(b) Cycle length is not less than $\overline{N}_1=(N_1/(N_1, N_2))$ since if $0\leqq K_1\neq K_2<\overline{N}_1$, then if K_1, K_2 correspond to the same cell $K_1K_2=a+pN_1$, $K_2N_2=a+qN_1$ and, subtracting $(K_1-K_2)N_2=(p-q)N_1$, we obtain $(K_1-K_2)\overline{N}_2(N_1, N_2)$ $=(p-q)\overline{N}_1(N_1, N_2)$ and $(K_1-K_2)\overline{N}_2=(p-q)\overline{N}_1$. However, since $\overline{N}_1=p_1^{\alpha_1}\cdots p_n^{\alpha_n}$ and $(\overline{N}_1, \overline{N}_2)=1$, all p_i must come from K_1-K_2; but $K_1-K_2<\overline{N}_1$ and hence all p_i cannot come from K_1-K_2, therefore $K_1-K_2=0$ and $p-q=0$, a contradiction.

COROLLARY. *For a single wrapping to be unique and cover completely, a necessary and sufficient condition is that cycle length* $=N_1$ *or that* $(N_1, N_2)=1$, i.e., N_1 and N_2 are relatively prime.

Returning to the case of multiple wrapping with multiplicity M, we note that the cycle length for a complete coverage must be $\geqq N_1/M$. This yields the condition for complete coverage in the following theorem:

THEOREM. *A necessary and sufficient condition for complete coverage is* $((N_1, N_2), M)=(N_1, N_2)$.

Proof. Length of cycle is $(N_1/(N_1, N_2))$, and the number of steps $=(N_1/M)$; hence $(N_1/(N_1, N_2))=K\cdot N_1/M$ for some integer K. Thus $(M/(N_1, N_2))=K$, so that (N_1, N_2) is a factor of M.

ON THE SOLUTIONS OF THREE ANCIENT PROBLEMS

EDWARD V. GRAEF, Pittsburgh, Pennsylvania and V. C. HARRIS, San Diego State College

It is well known that none of the problems of trisecting the angle, squaring the circle, and duplicating the cube can be solved using compass and straightedge alone. Here we use particular cases of the curves

$$(1)\qquad r=\sin\frac{\pi}{n}\csc\frac{\theta}{2k},\qquad n \text{ a positive integer} \geqq 2;\quad k=1, 2, 3, \cdots, n,$$

and

$$r = \lim_{n\to\infty} \sin\frac{\pi}{n}\csc\frac{\theta}{2n} = \lim_{n\to\infty}\left[\frac{2\pi}{\theta}\cdot\frac{\sin \pi/n}{\pi/n}\cdot\frac{\theta/2n}{\sin\frac{\theta}{2n}}\right] = \frac{2\pi}{\theta}, \tag{2}$$

to solve the three problems.

Let $k=n=3$ in (1); the single curve,

$$r = \sin\frac{\pi}{3}\csc\frac{\theta}{6},$$

suffices to trisect the angle. This is periodic with period 12π; we are interested in the domain $0<\theta<3\pi$ and indeed primarily in $0<\theta<(\pi/2)$. As θ goes from 0 to 3π we see that r goes from $+\infty$ to its minimum value $\sin \pi/3=\sqrt{3}/2$. This part of the curve winds around the pole $1\frac{1}{2}$ times. Also $r=1$ for $\theta=2\pi$. (See Figure 1.)

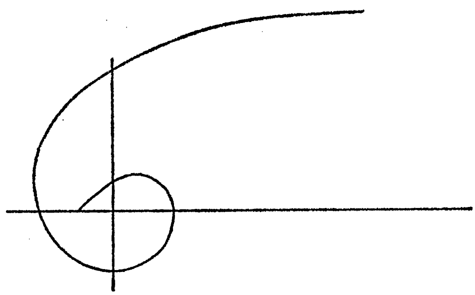


FIG. 1

An easy way to locate points on the curve is to draw any arc with O as center, intersecting the polar axis at S. Measure off three chords of length $2 \sin \pi/3$, counterclockwise, and the terminal point P of the third chord is a point of the curve. The converse is true and this enables the trisection to be accomplished. (See Figure 2.)

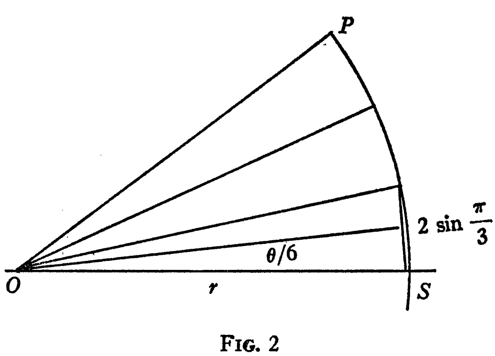


FIG. 2

Now let $\alpha<\pi/2$ be a given angle and construct an angle β congruent to α with vertex at the pole and initial side along the polar axis. Through the point P where the terminal side intersects the curve, for $\theta<(\pi/2)$ and with the pole as center, an arc is drawn intersecting the polar axis at S. Three chords of length $2 \sin \pi/3$ can be inscribed in arc PS and rays drawn from the pole to the endpoints of the chords trisect the angle. If the curves

$$r = \sin\frac{\pi}{3} \csc\frac{\theta}{2k}, \qquad k = 1, 2, 3,$$

are plotted, then the arc drawn as mentioned above is divided into three equal parts by the three curves and the angle is trisected. This is the only advantage of using curves with $k \neq n$.

Very easily the curve or curves

$$r = \sin\frac{\pi}{n} \csc\frac{\theta}{2n}; \qquad r = \sin\frac{\pi}{n} \csc\frac{\theta}{2k}, \quad k = 1, 2, \cdots, n,$$

can be used in an entirely similar fashion to divide the angle into $n \geqq 2$ equal parts. We have $r=1$, for $(\pi/n)=(\theta/2k)$ or $\theta=(2k\pi/n)$, $k=1, 2, \cdots, n$, Hence the n curves of one set pass thru the vertices of a regular n-gon inscribed in the unit circle. For purposes of multisecting the angle, the constant $\sin(\pi/n)$ could be replaced by any nonzero constant.

Evidently if the curves $r=\sin(\pi/n)\csc(\theta/2k)$ are available for $k=1, 2, \cdots, m$ they may be used to divide an angle into 1, 2, 3, $\cdots$, or m equal parts.

Now as $\theta \to 0$ the n chords inscribed in an arc with center the pole and with endpoints on the polar axis and on $r=\sin(\pi/n)\csc(\theta/2n)$ vary less in direction, and it is no surprise that

$$\lim_{\theta\to 0} y = \lim_{\theta\to 0} (r \sin\theta) = \lim_{\theta\to 0} 2n \sin\frac{\pi}{n} \frac{(\sin\theta)/\theta}{\left(\sin\frac{\theta}{2n}\right) \Big/ \theta/2n} = 2n \sin\frac{\pi}{n} \cdot$$

This is interpreted as the perimeter of a regular n-gon inscribed in the unit circle.

Attempting to square the circle, we use curve (2), namely, $r=2\pi/\theta$. Then

$$\lim_{\theta\to 0} y = \lim_{\theta\to 0} (r \sin\theta) = 2\pi \lim_{\theta\to 0} \frac{\sin\theta}{\theta} = 2\pi.$$

With a segment of length 2π and Euclidean tools a square of side $\sqrt{\pi}$ and area π can be constructed, thus squaring the circle of unit radius. Since however, $v=2\pi$ only when $r=\infty$, it is more convenient to proceed by inscribing chords of length $r=2n\sin(\pi/n)$ in circles of radius n tangent as indicated in Figure 3 to the 90° axis. Then $r=2n\sin(\pi/n)$, $\theta=(\pi/2)+(\pi/n)$; and so the equation of the curve is

$$r = 2\pi \frac{\sin\left(\theta - \frac{\pi}{2}\right)}{\theta - \pi/2} \cdot$$

The limit $\lim r_{\theta\to\pi/2}$ is 2π which solves the problem conveniently.

Now, to duplicate the cube, let L be a point (r, θ), with $\theta < \pi$, of the curve $r=\sin\pi/3 \csc\theta/2$ and denote by K the point $(r, 0)$. Chord LK has length

$2 \sin(\pi/3)$. (See Figure 4.) Locate M on line OK on the opposite side of O from K so that $OM=OK=OL=r$. Erect $MN \perp MK$ interesecting LK extended at N. On MK lay off KP with P on the same side of K as M so that $KP=(1/2)KN$. Erect a perpendicular to MK at P interesecting NK at Q. Let Q be the point (R, ϕ). Then for $\theta < \pi$,

$$\frac{OL}{PK} = \frac{2OL}{2PK} = \frac{MK}{KN} = \cos\left(\frac{\pi}{2} - \frac{\theta}{2}\right) = \sin\frac{\theta}{2},$$

since $\angle OKL = (\pi/2 - \theta/2)$. This gives

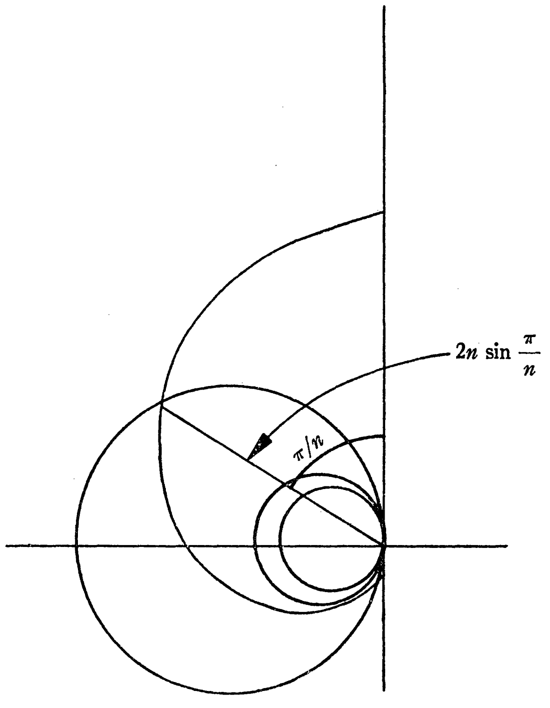


FIG. 3

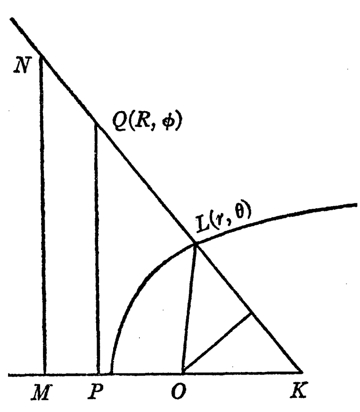


FIG. 4

$$\frac{r}{r + R\cos(\pi - \phi)} = \frac{\sin \pi/3}{r},$$

$$r^2 = \frac{\sqrt{3}}{2}r - \frac{\sqrt{3}}{2}R\cos\phi.$$

We find the intersection of the locus of points L on $r = \sin \pi/3 \csc \theta/2$ and points Q by setting $R = r = r_1$ and $\phi = \theta = \theta_1$. The preceding equation becomes

$$r_1^2 = \frac{\sqrt{3}}{2}r_1 - \frac{\sqrt{3}}{2}r_1\cos\theta_1,$$

so that

$$r_1 = \frac{\sqrt{3}}{2}(1 - \cos\theta_1) = \frac{\sqrt{3}}{2}\cdot 2\sin^2(\theta_1/2) = \sqrt{3}\sin^2(\theta_1/2).$$

But $\sin(\theta_1/2) = (\sin \pi/3)/r_1 = \sqrt{3}/2r_1$, so $r_1 = \sqrt{3}\cdot(3/4r_1^2)$ and $(2r_1)^3 = 8r_1^3 = 2(2\sin \pi/3)^3$. This shows that the cube of side $2r_1$ has twice the volume of the cube with side $2\sin \pi/3$. Thus the solution of the final one of the three famous problems has been accomplished.

COMBINATORIAL PROBLEMS IN SET-THEORETIC FORM

EDGAR M. PALMER, Michigan State University

1. Introduction. A fundamental problem in combinatorial mathematics is that of finding the size of various finite sets. These sets are often described by means of functions (mappings). When an equivalence relation is provided the problem becomes one of finding the number of equivalence classes of these functions.

In this article we shall consider three basic kinds of functions, (1) 1-1 functions, (2) arbitrary functions, and (3) onto functions. (Recall that a function f is 1-1 if for any two elements x_1 and x_2 in the domain, $f(x_1) = f(x_2)$ implies $x_1 = x_2$. A function f is *onto* if for every element y in the range, there is an element x in the domain such that $f(x) = y$.) By specifying three simple equivalence relations, we are confronted with nine elementary combinatorial problems. The solutions can all be expressed neatly in terms of the size of the domain and range.

As applications we obtain several basic combinatorial facts including the numbers of permutations and combinations with or without repetition. Each of the nine solutions can also be interpreted in various ways as the answer to an occupancy or distribution problem, i.e., the number of arrangements of objects in boxes.

The enumeration of equivalence classes of functions seems to provide a mathematically proper and natural setting for the study of permutations and combinations. Such an approach eliminates the ambiguity one often encounters when asked for the number of ways of placing balls in urns, objects in cells, beads in boxes, etc.

We assume that the reader is familiar with some of the elementary concepts of set theory, including functions and equivalence relations. Anyone who wishes to investigate combinatorial theory in more detail should find the excellent and complementary books by Riordan [2] and Ryser [**3**] and the exposition by deBruijn in [**1**] highly rewarding.

2. Equivalence relations for functions. Let $X=\{1, 2, \cdots, m\}$ and $Y=\{1, 2, \cdots, n\}$ be sets with m and n elements respectively; X is the domain and Y the range of the functions. As usual, we denote the set of all functions from X to Y by Y^X. Throughout this article, we shall use m and n to denote the orders of X and Y and furthermore we shall assume that m and n are not zero, i.e., X and Y are nonempty. Hence there is at least one function in the set Y^X.

We shall use the letters f, g, and h for functions in Y^X. A *permutation on a (finite) set* is a 1-1 function from that set to itself and we shall use the Greek letters α and β for permutations on X and Y. To eliminate parentheses, it is convenient to denote the image of an element x under a permutation α simply by αx.

We shall be concerned with three equivalence relations in Y^X, the first of which is equality, in which two functions f and g in Y^X are equal if they are identical. The second relation, called *domain equivalence*, is defined as follows. Two functions f and g in Y^X are *domain equivalent*, and we write $f\sim_d g$, if there is a permutation α on X such that for every x in X

$$f(\alpha x) = g(x). \tag{1}$$

In words, $f\sim_d g$ means that g can be obtained from f by permuting the elements of the domain X; the domain elements are exchangeable.

To see that domain equivalence is an equivalence relation, we first observe that if α is the identity map on X, then $f(\alpha x)=f(x)$ for all functions f. Hence $f\sim_d f$, so domain equivalence is reflexive.

Now suppose $f\sim_d g$, so that for some permutation α on X we may write $f(\alpha x)=g(x)$. Then if α^{-1} is the permutation inverse of α, $g(\alpha^{-1}x)=f(x)$ and thus $g\sim_d f$, establishing the symmetric property.

Finally, we assume $f\sim_d g$ and $g\sim_d h$. Then there are permutations α_1, and α_2 on X such that $f(\alpha_1 x)=g(x)$ and $g(\alpha_2 x)=h(x)$. But this implies that $f(\alpha_1\alpha_2 x)=h(x)$. Therefore $f\sim_d h$ and so domain equivalence is transitive.

The third relation in Y^X is called *range equivalence*. Two functions f and g in Y^X are *range equivalent*, and we write $f\sim_r g$, if there is a permutation β on Y such that for every x in X

$$\beta f(x) = g(x). \tag{2}$$

Thus in words, $f\sim_r g$ means that g can be obtained from f by permuting the elements of the range Y; the range elements are exchangeable. Clearly $\sim_r$ is an equivalence relation.

Note that equality, domain equivalence, and range equivalence are equivalence relations not only in Y^X but also in the subset of Y^X which consists of the 1-1 functions from X to Y. This follows from the observation that a function g, obtained by permuting the domain or range elements of a function f, is 1-1 if and only if f is also 1-1.

Similarly they are also equivalence relations in the subset of Y^X which consists of the functions from X *onto* Y.

3. The number of equivalence classes of functions. The number of equivalence classes of the three types of functions described earlier with respect to each of the three relations, $=$, $\sim_d$, and $\sim_r$, are stated in the propositions which follow. The results for each of the nine cases are displayed in the 3×3 table below (note that $S(m, n)$ denotes the "Stirling number of the second kind" (see [2] p. 33). Although the applications and interpretations for each proposition are numerous, we shall only present a few of the most important ones. We now proceed to justify the entries in the table.

TABLE: The number of equivalence classes of functions

type of function \ equivalence relation	$=$ equality	$\sim_d$ domain equivalence	$\sim_r$ range equivalence
1-1 functions $1 \leqq m \leqq n$	$n!/(n-m)!$	$\binom{n}{m}$	1
functions $m, n \geqq 1$	n^m	$\binom{n+m-1}{m}$	$\sum_{k=1}^{n} S(m, k)$
onto functions $m \geqq n \geqq 1$	$n!S(m, n)$	$\binom{m-1}{n-1}$	$S(m, n)$

PROPOSITION 1. *For* $m \leqq n$, *the number of* 1-1 *functions in* Y^X *is* $n(n-1)\cdots(n-m+1) = n!/(n-m)! = (n)_m$.

The proof of this proposition is immediate and the interpretations are numerous. An *m-permutation of n objects* is often defined as an ordered m-tuple of n objects without repetition. Since the latter are simply 1-1 functions, the number of m-permutations of n objects is $n!/(n-m)!$ When $m=n$, we obtain the familiar result that the number of permutations of n symbols is $n!$.

When we consider the elements of the range to be boxes and the elements of the domain to be objects of some sort, it is clear that $n!/(n-m)!$ is the number of arrangements of m different objects in n different boxes with at most one object in each box.

PROPOSITION 2. *For $m \leqq n$, the number of domain equivalence classes of* 1-1 *functions in Y^X is*

$$\binom{n}{m} = n!/((n-m)!m!).$$

The proof of the proposition consists of observing that if x is the number of such domain equivalence classes, then $m!x$ is the number of 1-1 functions, i.e., $m!x = n!/(n-m)!$.

An *m-combination of n objects* may be defined as an unordered m-tuple of n objects without repetition. The latter correspond precisely to the domain equivalence classes of 1-1 functions and hence their number is $\binom{n}{m}$. Similarly, the number of m-subsets of a set of n objects is $\binom{n}{m}$ as is also the number of arrangements of n objects in two different boxes with m objects in the first box and $n-m$ in the second. Finally, it is easy to see that $\binom{n}{m}$ is the number of arrangements of m similar (i.e., indistinguishable) objects in n different boxes with at most one object in each box.

PROPOSITION 3. *The number of arbitrary functions in Y^X is n^m.*

The proof of this proposition is also immediate. Since each function represents an ordered m-tuple of n objects with repetition, n^m is the number of m-permutations of n objects with repetition allowed.

If we interpret the range elements as boxes, n^m is the number of arrangements of m different objects in n different boxes. On the other hand, if the domain elements are boxes, n^m is the number of arrangements of n different objects in m different boxes with exactly one object in each box and with repetition allowed (i.e., the same object may occur in 0 through m boxes).

PROPOSITION 4. *The number of domain equivalence classes of functions in Y^X is*

$$\binom{n+m-1}{m}.$$

We will only sketch the proof of Proposition 4 which follows that given in [3, p. 9]. Each domain equivalence class corresponds to a sequence $y_1, y_2, \cdots, y_m$ of elements of Y with $y_i \leqq y_{i+1}$ for $i=1$ to $m-1$. Let S be the set $\{1, 2, \cdots, n+m-1\}$ of $n+m-1$ elements. Note that the set

$$\{y_1 + 0, y_2 + 1, \cdots, y_m + (m-1)\}$$

is an m-subset of S. Thus a 1-1 correspondence is determined between the domain equivalence classes and the m-subsets of S. Hence by Proposition 2, we have the required result.

Each of the classes here represents one of the m-combinations of n objects with repetition. Hence the number of the latter is

$$\binom{n+m-1}{m}.$$

Clearly

$$\binom{n+m-1}{m}$$

is also the number of arrangements of m similar objects in n different boxes, etc.

PROPOSITION 5. *For $m \geqq n$, the number of domain equivalence classes of onto functions in Y^X is*

$$\binom{m-1}{n-1}.$$

The number of such classes is the same as the number of domain equivalence classes of arbitrary functions from a set of $m-n$ domain elements into n range elements. Hence by Proposition 4 it is

$$\binom{n+(m-n)-1}{m-n} = \binom{m-1}{n-1}.$$

The most important application here is that

$$\binom{m-1}{n-1}$$

is the number of arrangements of m like (indistinguishable) objects in n different boxes with no box empty.

In order to state Propositions 6, 7, and 8, we shall use Stirling numbers, which are usually defined as follows (see [2] p. 33). For each integer $k \geqq 1$, let $(t)_k = t(t-1) \cdots (t-k+1)$, a polynomial of degree k in t, and set $(t)_0 = 1$. Since the polynomials $(t)_0, (t)_1, \cdots, (t)_i$ are linearly independent, the polynomial t^i can be expressed as their linear combination. In particular, let

$$t^i = \sum_{j=0}^{i} S(i,j)(t)_j. \tag{3}$$

The coefficients $S(i, j)$ in (3) are called *Stirling numbers of the second kind.* For convenience, let

$$S(i,j) = 0 \quad \text{unless} \quad i \geqq j \geqq 0 \tag{4}$$

It can be shown that

$$S(i,j) = S(i-1, j-1) + jS(i-1, j). \tag{5}$$

Hence $S(i, j)$ can be defined recurrently by (4), (5), and the initial condition $S(0, 0) = 1$.

PROPOSITION 6. *For $m \geqq n$, the number of onto functions in Y^X is $n!S(m, n)$.*

Let $F(m, n)$ be the number of onto functions and set $F(0, 0) = 1$. The onto functions may be classified according as the image of a specified element, say 1, of X is the image of 1 alone or not. In either case, the image can have n values.

In the first case, the remaining elements of X have $F(m-1, n-1)$ mappings; in the second they have $F(m-1, n)$ mappings. Hence we have the recurrence

$$F(m, n) = nF(m-1, n) + nF(m-1, n-1). \tag{6}$$

Using (4) and (5), it is easy to show that $n!S(m, n)$ satisfies the relation (6) for $F(m, n)$. Thus $F(m, n) = n!S(m, n)$.

It is clear that $n!S(m, n)$ is the number of arrangements of m different objects in n different boxes with no box empty.

The next two propositions follow readily from Proposition 6, so we simply state them and their occupancy interpretations.

PROPOSITION 7. *For $m \geqq n$, the number of range equivalence classes of onto functions in Y^X is $S(m, n)$.*

Thus $S(m, n)$ is the number of arrangements of m different objects in n similar boxes with no box empty.

PROPOSITION 8. *The number of range equivalence classes of arbitrary functions in Y^X is $\sum_{k=1}^{n} S(m, k)$.*

The occupancy problem solved here is the same as that for Proposition 7 except for the fact that empty boxes are allowed.

We complete the table by observing that all 1-1 functions are range equivalent. That is, for $m \leqq n$, there is only one arrangement of m different objects in n similar boxes with at most one object in each box.

Although we have only investigated elementary equivalence relations for functions, our approach sets the stage for solving more complicated problems. For example, the "necklace problem" asks for the number of different necklaces of m beads which can be made when an unlimited supply of beads of n different colors is available. This question, as well as many others, can be reformulated so that the problem is to find the number of equivalence classes of functions. Usually the equivalence relation is defined by means of permutation groups, and an explicit answer can be obtained by applying well known combinatorial methods, such as Pólya's enumeration theorem [2, p. 131].

Work supported in part by a grant from the National Science Foundation.

References

1. N. G. deBruijn, Pólya's Theory of Counting, Applied Combinatorial Mathematics, ed. by E. F. Beckenbach, Wiley, New York, 1964, pp. 144–184.

2. J. Riordan, An Introduction to Combinatorial Analysis, Wiley, New York, 1958.

3. H. J. Ryser, Combinatorial Mathematics, Carus Monograph 14, The Mathematical Association of America, 1963.

A NOTE ON NONHOMOGENEOUS EQUATIONS

Y. KUO, University of Tennessee

When we solve a homogeneous system of linear equations $zA = 0$, we need to find a basis of the solution space of the homogeneous system. Can we find a subset F of the solution set of a nonhomogeneous system of linear equations $xA=b$ over the real field R such that F forms something like a basis? The following theorem will answer the question. Let us start from the definitions. It is defined that a *flock combination* of the vectors $x_1, \cdots, x_n$ is a vector

$$x = c_1x_1 + \cdots + c_nx_n \qquad \text{where } c_k \in R, \quad \text{and} \quad \sum_k c_k = 1. \tag{1}$$

A subset S of a vector space is called a *flock* if, for any two elements of S, every flock combination of these elements also belongs to S.

Applying the concept of a basis to a flock, we can define the following:

A set H of elements of a flock S is called a *flock-basis* of S if, (i) every element of the flock S is a flock combination of H and (ii) no proper subset of H has this property.

It is easy to see that the solution set F' of $xA=b$ forms a flock. We will find a flock-basis of F' from the following theorem:

THEOREM. *If x^* is a solution of the system*

$$xA = b \tag{2}$$

and $\{z_1^*, \cdots, z_t^*\}$ is a basis of the solution space of the system $zA=0$, then $F=\{x^*, x^*+z_1^*, \cdots, x^*+z_t^*\}$ is a flock-basis of the solution set of (2).

Proof. The proof can be accomplished by the following two steps:

(a) Let F' be the flock of the solution set of (2). If $x^*+\sum_{k=1}^t c_kz_k^* \in F'$ where $c_k \in R$, then it is a flock combination of F. This follows from the fact that

$$x^* + \sum_k c_kz_k^* = \left(1 - \sum_k c_k\right)x^* + \sum_k c_k(z_k^* + x^*) \text{ with } 1 - \sum_k c_k + \sum_k c_k = 1.$$

(b) No proper subset of F has this property. In fact, if every solution $x^*+\sum_{k=1}^t c_kz_k$ of (2) is a flock combination of $F-\{x^*\}$, then there is a set of real numbers $\{d_k\}$ such that

$$x^* + \sum_{k=1}^t c_kz_k^* = \sum_{k=1}^t d_k(z_k^* + x^*),$$

with $\sum_{k=1}^t d_k=1$. Thus $(1-\sum_k d_k)x^*+\sum_k (c_k-d_k)z_k^*=0$. However, from $1-\sum_k d_k=0$ and the fact that z_k^* are linearly independent, it follows that $c_k=d_k$ for all k. Since z_k^* were arbitrary real numbers, we have a contradiction. Therefore, $x^*+\sum_k c_kz_k^*$ is not a flock combination of $F-\{x^*\}$.

Similarly, if $x^*+\sum_k c_kz_k^*$ is a flock combination of $F-\{x^*+z_j^*\}$, then we have

$$x^* + \sum_{k=1}^t c_kz_k^* = \sum_{k\neq j} d_k(z_k^* + x^*) + d_0x^*,$$

where $\sum_{k\neq j} d_k+d_0=1$. Thus $\sum_{k=1}^t c_kz_k^* = \sum_{k\neq j} d_kz_k^*$. But, since z_k^* are linearly independent, this yields $c_j=0$, and $c_k=d_k$ for $k\neq j$. However, since c_j was arbitrary, we have a contradiction. Therefore, $x^*+\sum_k c_kz_k^*$ is not a flock combination of $F-\{x^*+z_j^*\}$. This shows that F is a flock-basis of the solution set of (2).

If we also consider a finite dimensional vector space V over the real field R from the point of view of affine geometry, then the relation between this paper and [1] can be made as follows:

A *flock combination* x *of* $x_1, \cdots, x_n$ in (1) is the *centroid* of the points $x_1, \cdots, x_n$ with weights $c_1, \cdots, c_n$, and a *flock* S is an *affine subspace* of V. If $H=\{x_1, \cdots, x_n\}$ is a set of *affinely independent points* and S is the affine subspace spanned by H, then H is called an *affine-basis* of S. It is easy to see that a *flock-basis* H of a flock S is an *affine-basis* of the affine subspace S spanned by H. In the theorem of this paper, the set of solutions of (2) is the affine subspace spanned by an affine-basis $F=\{x^*, x^*+z_1^*, \cdots, x^*+z_t^*\}$. Therefore, every solution x of (2) has a unique representation as a centroid of points of F. Consequently, every solution x of (2) has a unique expression as a flock combination of elements of F.

The author wishes to thank the referee and the editor for their suggestions and comments.

References

1. Garrett Birkhoff and Saunders MacLane, A Survey of Modern Algebra, 2nd ed., Macmillan, New York, 1953, pp. 287–292.

2. Arno Jaeger, Introduction to Analytic Geometry and Linear Algebra, Holt, Rinehart and Winston, New York, 1960.

3. H. W. Kuhn and A. W. Tucker (eds.), Linear Inequalities and Related Systems, Princeton University Press, 1956.

A NOTE ON EUCLID'S ALGORITHM

YONG-JENG LEE, Emory University

1. Introduction. An important theorem states that:

Let a and b be positive integers and let $d=(a, b)$, the greatest common divisor of a and b; then there exist integers M and N such that

$$(a, b) = Ma + Nb.$$

The purpose of this note is to give an algorithm for simultaneously determining (a, b), M, and N.

2. Algorithm. Apply the Euclidean algorithm to a and b to obtain the equations

$$\begin{array}{ll} a = bq_1 + r_1 & 0 < r_1 < b \\ b = q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 = q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ \cdots\cdots\cdots & \\ r_{n-2} = q_n r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n & \end{array}$$

Define $s_1=(a+1)-bq_1$, $s_2=b-s_1q_2$ and for $j>2$, $s_j=s_{j-2}-s_{j-1}q_j$, $t_1=a-(b+1)q_1$, $t_2=(b+1)-t_1q_2$ and for $j>2$, $t_j=t_{j-2}-t_{j-1}q_j$.

By induction, we have the following theorem and its corollary.

THEOREM. $r_j=(s_j-r_j)a+(t_j-r_j)b$.

COROLLARY. $(a, b)=(s_n-r_n)a+(t_n-r_n)b$.

This corollary gives rise to the algorithm. As an illustration, we consider the following example:

Example. Find (630, 132) and express it in the form $630M+132N$.

	a	$a+1$	a	b	b	$b+1$	
	630	631	630	132	132	133	$4=q_1$
	528	528	532	102	103	98	
	r_1	s_1	t_1	r_2	s_2	t_2	
$q_2=1$	102	103	98	30	29	35	$3=q_3$
	90	87	105	24	32	-14	
	r_3	s_3	t_3	r_4	s_4	t_4	
$q_4=2$	12	6	-7	6	-3	49	$2=q_5$
	12						
	0						
	Stop						

$(a, b)=r_4=6$; $M=s_4-r_4=-3-6=-9$; $N=t_4-r_4=49-6=43$.

Hence $(a, b)=(s_4-r_4)a+(t_4-r_4)b$; $6=(-9)630+(43)132$.

The author is indebted to the referee for simplifying the mathematical development. The author was supported by University Fellowship.

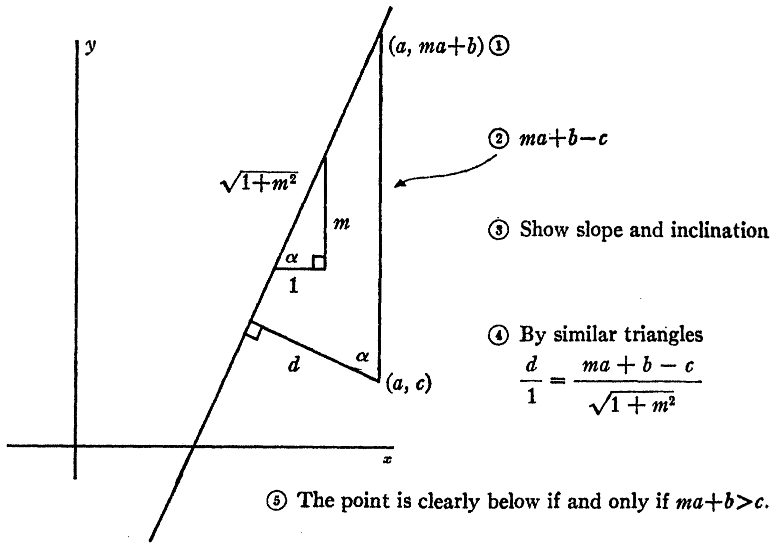
AN EASY WAY FROM A POINT TO A LINE

R. L. EISENMAN. Office of Secretary of Defense, Systems Analysis and Air Force Academy

We should and do publicize the use of coordinate geometry for concise proofs in synthetic geometry. Do we recognize that synthetic geometry can return the favor? This note suggests such an application to derive the distance from a point to a line via similar triangles.

In its fancier dress as "orthogonal projection," distance from a point to a line is a forerunner for orthogonal functions and it is a working tool in such applications as interpreting measures of good fit in statistics.

We usually prove distance from (a, c) to $y=mx+b$ is $(ma+b-c)/\sqrt{1+m^2}$ by intricate algebra to locate the foot of the perpendicular, and end with a discussion of the significance of the algebraic sign. Consider instead this basic diagram with the numbered observations following in turn:



The symmetric version, $a_1x+a_2y+a_3=0$, is useful for extension to more dimensions. Perhaps the students would enjoy formulating an educated guess of the formulas for distances in a general number of dimensions.

FACTORIZATION OF $x^{2n}+x^n+1$ USING CYCLOTOMIC POLYNOMIALS

BRYANT TUCKERMAN, IBM Watson Research Center

Salkind [1] has given some interesting conditions for the polynomial $x^{2n}+x^n+1$ to have divisors $x^2\pm x+1$ and $x^{6s}\pm x^{3s}+1$, the proofs using cube roots of unity. (We write x instead of a.)

Each of these polynomials is a divisor of some $x^m\mp 1$, in fact is a finite geometric series in some $\pm x^b$ with one terminal term $+1$, which in turn is (except perhaps for a factor -1) a quotient $(x^{cb}\mp 1)/(x^b\mp 1)$.

The aim of this note is to call attention to the effectiveness of cyclotomic polynomials [2, 3] in the study of such divisors of $x^m\mp 1$. The *cyclotomic polynomial* $F_n(x)$ is the (unique, irreducible) monic polynomial whose roots are simple and are all the primitive nth roots of unity. Particular cases are the above expressions $x^2+x+1=(x^3-1)/(x-1)=F_3(x)$, $x^2-x+1=(x^3+1)/(x+1)=F_6(x)$. A well-known relation, $x^m-1=\prod_{d\mid m} F_d(x)$, expresses any x^m-1 as a product of certain $F_d(x)$. (Here, $j\mid k\,[j\nmid k]$ means that j does [does not] divide k.) Any x^m+1 can also be expressed, a little less simply, as a product of certain $F_d(x)$, since $x^m+1=(x^{2m}-1)/(x^m-1)$. Another useful formula [2, 3], not needed here, conversely expresses any $F_n(x)$ as a quotient of two products of certain x^e-1.

In the present problem, writing $x^{2n}+x^n+1=S_n(x)$ for brevity, we see that

$$S_n(x) = (x^{3n}-1)/(x^n-1) = \Big(\prod_{d|3n} F_d(x)\Big)\Big/\Big(\prod_{d|n} F_d(x)\Big)$$

$$= \prod_{\substack{d|3n \\ d\nmid n}} F_d(x) = \prod_{d'|n'} F_{3^{a+1}\cdot d'}(x),$$

where $n=3^a\cdot n'$, $a\geqq 0$, $3\nmid n'$, $d=3^{a+1}\cdot d'$. This immediately gives the complete unique factorization (depending on n) of $S_n(x)$ into irreducible polynomials $F_d(x)$.

Using the above notation and formula, we can pose and directly answer typical questions about divisors of $S_n(x)$. For example, the following are roughly, reformulations of the questions treated in [1].

(1) When does x^2+x+1 divide $S_n(x)$?

Answer. $(F_3(x)\,|\,S_n(x)) \Leftrightarrow (3=d=3^{a+1}\cdot d'$ for some $d'\,|\,n') \Leftrightarrow (a=0$ and $1\,|\,n') \Leftrightarrow (n\not\equiv 0 \pmod 3))$.

(2) When does x^2-x+1 divide $S_n(x)$?

Answer. $(F_6(x)\,|\,S_n(x)) \Leftrightarrow (6=d=3^{a+1}\cdot d'$ for some $d'\,|\,n') \Leftrightarrow (a=0$ and $2\,|\,n') \Leftrightarrow (n\not\equiv 0 \pmod 3)$ and $n\equiv 0 \pmod 2))$.

(3) When is $S_n(x)$ irreducible?

Answer. $(S_n(x)$ is irreducible$) \Leftrightarrow (d$ is unique$) \Leftrightarrow (d'$ is unique$) \Leftrightarrow (n'=1) \Leftrightarrow (n=3^a$ (for some $a\geqq 0$)$) \Leftrightarrow (n=1, 3, 9, 27, \cdots)$.

All other $S_n(x)$ are reducible. Example:

$$S_{15}(x) = x^{30}+x^{15}+1 = F_9(x)\cdot F_{45}(x)$$
$$= (x^6+x^3+1)\cdot(x^{24}-x^{21}+x^{15}-x^{12}+x^9-x^3+1).$$

This treatment in terms of cyclotomic polynomials suggests generalizations. For example, the present problem is the case $p=3$, $S_n(x)=G_3(x^n)$ of the divisibility of $x^{(p-1)n}+x^{(p-2)n}+\cdots+x^2+x+1=G_p(x^n)=(x^{pn}-1)/(x^n-1)$ by $x^{p-1}\pm x^{p-2}+\cdots+x^2\pm x+1=G_p(\pm x)=(x^p\mp 1)/(x\mp 1)$ for odd p, where, by definition, $G_k(y)=y^{k-1}+y^{k-2}+\cdots+y+1$. When p is furthermore prime, it can be shown by replacing 3 by p in the above arguments that: n.a.s.c. for $G_p(x^n)$ to be divisible by

$$\begin{Bmatrix} G_p(+x) \\ G_p(-x) \end{Bmatrix} \text{ are that } \begin{Bmatrix} n \not\equiv 0 \pmod p \\ n\not\equiv 0 \pmod p \;\&\; n\equiv 0 \pmod 2 \end{Bmatrix};$$

n.a.s.c. that $G_p(x^n)$ is irreducible is that $n=p^a$ for some $a\geqq 0$.

References

1. C. T. Salkind, Factorization of $a^{2n}+a^n\times 1$, this MAGAZINE, 38 (1965) 163.

2. Trygve Nagell, Introduction to Number Theory, Wiley, New York, 1951, Chapter 5.

3. D. H. Lehmer, Some properties of the cyclotomic polynomial, J. Math. Anal. Appl., 15 (1966) 105–117.

PROBLEMS AND SOLUTIONS

EDITED BY ROBERT E. HORTON, Los Angeles Valley College

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. 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.

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 Robert E. Horton, Los Angeles Valley College, 5800 *Fulton Avenue, Van Nuys, California* 91401.

To be considered for publication, solutions should be mailed before June 1, 1969.

PROBLEMS

712. *Proposed by C. R. J. Singleton, Petersham, Surrey, England.*

A four-digit number is equal to the product of three numbers of one, two, and three digits, respectively. The ten digits of these four numbers are all different. Find the two solutions.

713. *Proposed by Brother Alfred Brousseau, St. Mary's College, California.*

An examination was prepared as follows. Thirty-six questions were made and each assigned a number corresponding to the figures that might come up using two differentiated dice. Contestants were given questions by throwing the two dice. If the number that came up belonged to a question already used, the throw was repeated. What would be the expected number of throws needed to select all thirty-six questions?

714. *Proposed by Samuel Wolf, Linthicum Heights, Maryland.*

Find a solution in base 12 for

$$\begin{array}{rrrrrrr} & V & I & O & L & I & N \\ & V & I & O & L & I & N \\ & & V & I & O & L & A \\ & & C & E & L & L & O \\ \hline Q & U & A & R & T & E & T \end{array}$$

715. *Proposed by John Brillart, Berkeley, California.*

Given the classical 3×3 magic square

$$M = \begin{pmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{pmatrix}$$

Compute M^n for $n \geqq 2$.

716. *Proposed by John M. Howell, Los Angeles City College.*

Suppose that we have a deck of cards numbered 1, 2, $\cdots$ n and a second deck numbered 1, 2, $\cdots$ $(n+d)$, $d \geqq 0$, and that we shuffle the two decks and draw one card at a time from each until the smaller deck is exhausted. Find the probability of r matching draws and the mean and variance of the number of matching draws.

717. *Proposed by V. F. Ivanoff, San Carlos, California.*

In a convex pentagon we are given the areas of five triangles each formed with two sides and one diagonal. Find the areas of the remaining five triangles each formed with one side and two diagonals.

718. *Proposed by A. H. Lumpkin, East Texas State University.*

In $R \times R$ with the usual metric, if G is an infinite subset of $R \times R$ such that for all x, y in G, $d(x, y)$ is an integer, then $G \subseteq l$ for some line l.

SOLUTIONS

Late Solutions

Paul Sugarman, Swampscott, Massachusetts: **677, 679,** *and* **683;** *Andrzej Makowski, Warsaw, Poland:* **674;** *Heiko Harborth, Braunschweig, Germany:* **679, 682,** *and* **683.**

A Product of Integers

691. [May, 1968] *Proposed by Charles W. Trigg, San Diego, California.*

Using the nine positive digits just once each, form two integers A and B such that $A = 8B$.

Solution by Edward Moylan, Ford Motor Company, Dearborn, Michigan.

Obviously A has 5 digits and B has 4 digits. Since A is a multiple of 8, its units digit is even, its last two digits form a multiple of 4, and its last three digits form a multiple of 8.

Suppose the units digit of A is 2, then the units digit of B is either 4 or 9. Choose 9. Now the tens digit of A must be odd. Choose 1. Now the tens digit of B must be 6. The hundreds digit of A is 3, 5, 7, or 9. Only 9 will yield a valid answer. It is $A = 58912$ and $B = 7364$. Actually there are 46 such combinations. I only derived one of these by hand. The rest are computer generated.

A	B	A	B
25496	3187	46312	5789
36712	4589	46328	5791
36728	4591	46712	5839
37512	4689	47136	5892
37528	4691	47328	5916
38152	4769	47368	5921
41896	5237	51832	6479
42968	5371	53928	6741

A	B	A	B
54312	6789	71456	8932
54328	6791	71536	8942
54712	6839	71624	8953
56984	7123	71632	8954
58496	7312	73248	9156
58912	7364	73264	9158
59328	7416	73456	9182
59368	7421	74528	9316
63152	7894	74568	9321
63528	7941	74816	9352
65392	8174	75328	9416
65432	8179	75368	9421
67152	8394	76184	9523
67352	8419	76248	9531
67512	8439	76328	9541

Also solved (complete with 46 pairs) by David C. Daykin, University of Malaya; Monte Dernham, San Francisco, California; John W. Pittman, Greenbelt, Maryland; W. J. Sonsin, Edgewood Arsenal, Maryland; M. I. Urusemeyer, Soest, the Netherlands; and the proposer.

Partial solutions (1 to 45 pairs) were submitted by Merrill Barnebey, Wisconsin State University at Lacrosse; Gladwin E. Bartel, Washington State University; Ronald L. Browning, Geneseo College, New York; David S. Chernoff, Los Angeles, California; Charles R. Conniff, Southern Illinois University; Charles Fleenor, Ball State University; Anton Glaser, Pennsylvania State University, Abington, Pennsylvania; Michael Goldberg, Washington, D. C.; Louise S. Grinstein, New York, New York; Larry Hansen, Lakehead University, Port Arthur, Canada; H. Fred Hassenphig, Winthrop College, South Carolina; Philip Haverstick, Liberty, Missouri; J. A. H. Hunter, Toronto, Canada; Richard Kuszpa, University of Connecticut; Peter A. Lindstrom, Genesee Community College, New York; Douglas Lind, Vanderbilt University; Otto Mond, White Plains, New York; Rachel H. Netzband, Cazenovia College, New York; G. A. Novacky, Jr., Wheeling College, Pennsylvania; Bernard J. Portz, Jesuit College, Minnesota; John E. Prussing, University of California at San Diego; Anthony Quaglia, W. H. Sadler, Inc., New York; Paul Sugarman, Massachusetts Institute of Technology; Howard L. Walton, Decision Studies Group, Washington, D. C.; Kenneth M. Wilke, Topeka, Kansas; Gordon Woulff, Bronx High School of Science, New York; Gregory Wulczyn, Bucknell University; and K. L. Yocom, South Dakota State University.

D. Sumner, Montreal, Canada, made the assumption that all nine integers must appear in both A and B. His solution follows.

Let $B_1=123456789$ and $A_1=987654321$. Clearly B_1 and A_1 are respectively the smallest and largest integers that can be written using the nine positive digits once each. Thus the possible A's are those 9-digit integers divisible by 8, less than A_1 and greater than or equal to $8B_1$.

Now $8B_1=987654312$ is just 9 less than A_1 so there are only two possible A's, namely $8B_1=987654312$ and $8B_1=987654320$. Clearly the first uses all nine positive digits and it is 8 times B_1 which satisfies the initial requirement. Thus $A=987654312$ and $B=123456789$ and these are the only solutions to the problem as stated.

Also solved under this assumption by George Fabian, Park Forest, Illinois; Paul Funkenbusch, Fifth Grade, Houghton, Michigan; Ned Harrell, Menlo-Atherton High School, California; Lew Kowarski, Morgan State College, Maryland; and James R. Kuttler, Johns Hopkins University, Applied Physics Laboratory. One solution was received with an undecipherable signature.

Factorial Sum

692. [May, 1968] *Proposed by Michael J. Martino, Temple University.*

Prove that $1!+2!+3!+\cdots+k!$ is asymptotic to $(k+1)!/k$ as $k\to\infty$.

Solution by John E. Prussing, University of California at San Diego.

To show that the series $1!+2!+3!+\cdots+k!$ is asymptotic as $k\to\infty$ to $(k+1)!/k$ (which happens to be the sum of the last two terms of the series), one must demonstrate that

$$\lim_{k\to\infty} k/(k+1)![k!+(k-1)!+(k-2)!+\cdots+1!]=1$$

This limit simplifies to:

$$\lim_{k\to\infty} k\left[\frac{1}{k+1}+\frac{1}{(k+1)k}+\frac{1}{(k+1)k(k-1)}+\cdots+\frac{1}{(k+1)!}\right]$$

or

$$\lim_{k\to\infty}\left[\frac{k}{k+1}+\frac{1}{k+1}+\frac{1}{(k+1)(k-1)}+\cdots+\frac{1}{(k+1)(k-1)!}\right]=1$$

Also solved by Sister Marion Beiter, Rosary Hill College; Nicholas C. Bystrom, Northland College, Wisconsin; George Fabian, Park Forest, Illinois; James Geer, IBM Corporation, Endicott, New York; Michael Goldberg, Washington, D. C.; Robert J. Herbold, Procter and Gamble Company, Cincinnati, Ohio; Ignacio D. Herssein, City College of New York; Erwin Just, Bronx Community College; Lew Kowarski, Morgan State College, Maryland; Norbert J. Kuenzi, Iowa City, Iowa; Douglas Lind, Vanderbilt University; R. S. Luthar, University of Wisconsin at Waukesha; Terry Mackin, Hamline University; Hugh Noland, Chico State College, California; Anthony Quaglia, W. H. Sadlier, Inc., New York; Henry J. Ricardo, Yeshiva University; Ellis J. Rich, Maritime College, New York; B. E. Rhoades, Indiana University; E. P. Starke, Plainfield, New Jersey; K. L. Yocom, South Dakota State University. One incorrect solution was received.

Log Log Paper

693. [May, 1968] *Proposed by Stanley Rabinowitz, Far Rockaway, New York.*

A square sheet of one cycle by one cycle log log paper is ruled with n vertical lines and n horizontal lines. Find the number of perfect squares on this sheet of logarithmic graph paper.

Solution by the proposer.

If x and y axes are set up, the lines meet these axes at the points log 1, log 2, log 3, $\cdots$ log n for a proper choice of the logarithmic base. For a square to exist, we must have $\log a-\log b=\log c-\log d$ or $a/b=c/d$ where a, b, c, and d are integers less than or equal to n with $a\neq b$.

For any $a\neq 1$, there are $\phi(a)$ choices for $b<a$ such that a/b is in lowest terms. For any such a/b, the number of fractions whose numerators and denominators are in the allowed range which are equal to a/b is $[n/a]$, where $[x]$ denotes the greatest integer in x. We may pair any one with any other one (including itself) to get a square on the graph paper. So for any a/b, the number of squares obtained is $[n/a]^2$.

Multiplying by the $\phi(a)$ choices for b and summing over all $a\neq 1$, we find that the total number of squares is

$$\sum_{a=2}^{n} [n/a]^2\phi(a).$$

Also solved by Michael Goldberg, Washington, D. C.

An Old Triangle Problem

694. [May, 1968] *Proposed by J. S. Vigder, Defence Research Board of Canada, Ottawa, Canada.*

Find all the triangles with integral sides in which the area and perimeter are equal to the same integer.

Solution by E. P. Starke, Plainfield, New Jersey.

In the usual notation, we have from the hypothesis

$$2s = \sqrt{s(s-a)(s-b)(s-c)}. \tag{1}$$

With $x=s-a$, $y=s-b$, $z=s-c$, $s=x+y+z$, (1) becomes

$$4(x+y+z) = xyz. \tag{2}$$

Suppose (without loss of generality) $x \leqq y \leqq z$. Then $3<x$ implies $xyz \geqq 16z$ and $x+y+z \leqq 3z$, so that

$$4(x+y+z) \leqq 12z < 16z \leqq xyz$$

and (2) would be impossible. Hence we need try only $x=1, 2, 3$.

For $x=1$, (2) becomes $(y-4)(z-4)=20$, whence $y=5$, $z=24$; $y=6$, $z=14$; $y=8$, $z=9$.

For $x=2$, (2) becomes $(y-2)(z-2)=8$, whence $y=3$, $z=10$; $y=4$, $z=6$.

For $x=3$, (2) gives $(3y-4)(3z-4)=52$. Now y cannot be 3 since $3y-4=5$ is not a factor of 52. y cannot be greater than 3 since $4 \leqq y \leqq z$ implies $8 \leqq 3y-4 \leqq 3z-4$, whence $(3y-4)(3z-4) \geqq 64$, a contradiction.

From the values of x, y, z listed, we have the five solutions: $a, b, c = 6, 25, 29$; $7, 15, 20$; $9, 10, 17$; $5, 12, 13$; $6, 8, 10$.

Also solved by Merrill Barnebey, Wisconsin State University at LaCrosse (partially); Hugh M. Edger, San Jose State College; George Fabian, Park Forest, Illinois (partially); Michael Goldberg, Washington, D. C.; B. McMillan, Morgan State College, Maryland; M. T. Urusemeyer, Soest, The Netherlands; Kenneth M. Wilke, Topeka, Kansas; Gregory Wulczyn, Bucknell University (partially); K. L. Yocom, South Dakota State University; and the proposer.

J. A. H. Hunter pointed out that he had previously published the problem and its solution in the December, 1961, issue of the magazine, *Saturday Night*, and again in his book, *Mathematical Diversions*, Van Nostrand, Princeton, New Jersey, 1963. Michael Goldberg found the problem and solution by Whitworth and Biddle in Math. Ques. Ed. Times, 5 (1904) 54–56 and 62. Two incorrect solutions were received.

An Exhaustive Drawing

695. [May, 1968] *Proposed by John M. Howell, Los Angeles City College.*

A population consists of a items of type A and b items of type B. One at a time is drawn without replacement until all of the type A items are drawn.

What is the probability that this happens on the xth draw where $x=a, a+1, \cdots, a+b$?

Solution by Norbert J. Kuenzi, Iowa City, Iowa.

As a model, consider sequences of A's and B's of length $a+b$ in which there are exactly a A's and b B's. Such a sequence with the ath A in the xth position represents a sequence of drawings which terminate at the xth draw.

There are

$$\binom{a+b}{a}$$

such sequences. Assign probability

$$1/\binom{a+b}{a}$$

to each. For $x=a, a+1, \cdots, a+b$ consider sequences which represent the ath type A item being drawn on the xth draw. Clearly any sequence of this type has an A in the xth position and $(a-1)$ A's in the first $(x-1)$ positions. There are

$$\binom{x-1}{a-1}$$

such sequences.

Hence the probability that the ath type A item is drawn on the xth draw, where $x=a, a+1, \cdots, a+b$ is

$$\binom{x-1}{a-1}\Big/\binom{a+b}{a}$$

which can be written

$$a(b!)(x-1)!/(x-a)!(a-b)!.$$

Also solved by Gladwin E. Bartel, Washington State University; Melvin Billik, New York University; Robert X. Brennan, Basel, Switzerland; George Fabian, Park Forest, Illinois; W. W. Funkenbusch, Michigan Technological University; Michael Goldberg, Washington, D. C.; Philip Haverstick, Liberty, Missouri; James C. Hickman, University of Iowa; B. McMillan, Morgan State College, Maryland; Hugh Noland, Chico State College, California; Kenneth A. Ribet, Brown University; Paul Sugarman, Massachusetts Institute of Technology; M. T. Urusemeyer, Soest, The Netherlands; Julius Vogel, Newark, New Jersey; Howard L. Walton, Decision Studies Group, Washington, D. C.; K. L. Yocom, South Dakota State University; and the proposer.

W. W. Funkenbusch noted that this problem is related to Problem 142, March, 1953, page 219, proposed by George Pate. A simple transformation of the letters used by Funkenbusch in his solution to Problem 142 will produce the solution to Problem 695.

Elliptical Section

696. [May, 1968] *Proposed by H. W. Vayo and R. W. Shoemaker, University of Toledo.*

Given a prolate spheroidal surface, if one rotates the transverse midsection about the minor axis, one obtains an elliptical section on the surface. Find an expression for the length of the semimajor axis of this ellipse in terms of the angle of rotation and also an expression for the eccentricity of the ellipse.

Solution by the proposers.

The upper half of the spheroid is $(x^2+y^2)/r^2+4z^2/1^2=1$, where r is semiminor axis of spheroid and 1 is major axis of spheroid. Express this in spherical coordinates: $\rho^2 \sin^2 \phi/r^2+4\rho^2 \cos^2 \phi/a^2=1$, where ρ is semimajor axis of ellipse and ϕ is azimuth angle. Now we know that for some angle of rotation γ_0: $\phi_0+\gamma_0 =\Pi/2$. We substitute $\phi=\phi_0$ into the expression in spherical coordinates to obtain

$$\rho = \frac{ra}{[a^2 \sin^2(\Pi/2 - \gamma_0) + 4r^2 \cos^2(\Pi/2 - \gamma_0)]1/2},$$

where length of major axis of spheroid is a. The eccentricity is clearly $\sqrt{(\rho^2-r^2)}\rho$.

Also solved by Michael Goldberg, Washington, D. C.

Application of Rolle's Theorem

697. [May, 1968] *Proposed by Erwin Just, Bronx Community College.*

Assume that each member of the sequence of functions $f_1, f_2, \cdots, f_n$ is differentiable on $[a, b]$, $f_1(a)=f_n(b)=0$ and $f_i(x)\neq 0$ when $x\in(a, b)$, $i=1, 2, \cdots, n$. Prove that there exists $c\in(a, b)$ such that $\sum_{i=1}^n f_i'(c)/f_i(c)=0$.

Solution by Gesing Leung, Hong Kong.

Let $f=f_1 \cdots f_n$ so that $f(x)=f_1(x) \cdots f_n(x)$ for all $x\in[a, b]$. Then f is differentiable on $[a, b]$, $f(a)=f(b)=0$ and $f(x)\neq 0$ for $x\in(a, b)$. So by Rolle's theorem there exists $c\in(a, b)$ with $f'(c)=0$.

Now for $x\in(a, b)$,

$$\begin{aligned} f'(x) &= \sum_{i=1}^n f_1(x) \cdots f_{i-1}(x)f_i'(x)f_{i+1}(x) \cdots f_n(x) \\ &= f(x) \sum_{i=1}^n \frac{f_i'(x)}{f_i(x)} \end{aligned}$$

In particular,

$$f'(c) = f(c) \sum_{i=1}^n \frac{f_i'(c)}{f_i(c)}\cdot$$

As $c\in(a, b)$, $f(c)\neq 0$; but $f^1(c)=0$, so

$$\sum_{i=1}^n \frac{f_i'(c)}{f_i(c)} = 0.$$

Also solved by Donald Batman, MIT, Lincoln Laboratory; Richard J. Bonneau, Holy Cross

College; Wray G. Brady, University of Bridgeport; Robert J. Bridgman, Mansfield State College, Pennsylvania; John L. Brown, Jr., Ordnance Research Laboratory, State College, Pennsylvania; Julio Cano, University of Toledo, Ohio; D. R. Chand and S. S. Kapur, Lockheed-Georgia Company; W. G. Dotson, Jr., North Carolina State University; Michael Goldberg, Washington, D. C.; Marvin Gruber, Rochester Institute of Technology; Larry Hansen, Lakehead University, Port Arthur, Ontario; Robert J. Herbold, Procter and Gamble Company, Cincinnati, Ohio; Norbert J. Kuenzi, Iowa City, Iowa; Douglas Lind, University of Virginia; Peter A. Lindstrom, Genesee Community College, New York; Terry Mackin, Hamline University; B. McMillan, Morgan State College, Maryland; Edward Moylan, Ford Motor Company, Dearborn, Michigan; Rachel M. Netzband, Cazenovia College, New York; Willis B. Porter, New Iberia, Louisiana; B. E. Rhoades, Indiana University; Kenneth A. Ribet, Brown University; Henry J. Ricardo, Yeshiva University; W. M. Sanders, Lawrence University, Wisconsin; W. J. Sonsin, Edgewood Arsenal, Maryland; Jack E. Slingerland, Portland State College, Oregon; William Stewart, Xavier University, Ohio; Dimitrios Vathis, Chalcis, Greece; Howard L. Walton, Decision Studies Group, Washington, D. C.; K. L. Yocom, South Dakota State University; and the proposer. One unsigned solution was received.

Comment on Problem 635

635. [November, 1966, and May, 1967] *Proposed by P. D. and R. L. Goodstein, University of Leicester, England.*

Show that there is a closed path along the edges of a regular dodecahedron which divides the dodecahedron into two congruent parts each of which contains a pair of opposite faces of the dodecahedron.

Comment by Charles W. Trigg, San Diego, California.

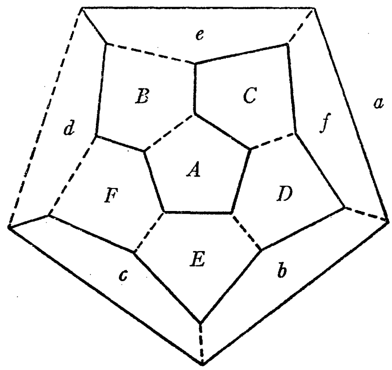
Indicate one face of the dodecahedron by A, those adjacent to it by B, C, D, E, F lettered consecutively and clockwise, and the faces opposite these by the corresponding lower case letters.

If the dodecahedron is divided into two congruent parts by cutting along the edges, the two parts will have a perimeter in common which will constitute a closed path, provided that no edge is traversed twice.

The method used in the solution published on Page 164 of the May, 1967, issue, produces a closed path 10 edges long which divides the dodecahedral surface into two congruent parts that contain *no opposite faces*. Indeed if the downward path be started from the vertex common to B, d, and e, going between B and e, the two parts will consist of $ABCDEF$ and $abcdef$. When five edges of each part are slit, the parts may be flattened out into the net of the dodecahedron which is usually shown.

However, there are closed paths which accomplish the desired dissection.

Method I. The surface of the dodecahedron may be divided into two congruent strips in two essentially different ways, $ABefbc-adFEDC$ and $ABdcbf-aeCDEF$. These strips of six pentagons joined edge to edge have perimeters which are closed paths 20 edges long. They may be flattened into a plane. Each part contains *one pair* (and only one) of opposite faces. The parts from the first dissection are mirror images of the parts from the second dissection. The two strips of the first dissection are shown on the accompanying Schlegel diagram in which the closed path is shown in solid lines.



Method II. Starting with three faces at a vertex, a strip of three faces may be appended in two essentially different ways to produce two congruent parts, *ABCfac—DbEFde* and *ABCfbc—aedFED*. In each case, the two parts have a common perimeter 18 edges long. One of the vertex edges will be split in order to flatten out the part. Each part contains *two pairs* of opposite faces.

Method III. Starting with three faces at one vertex, another vertex may be chosen which has two faces having edges in common with one of the original faces. This may be done in two ways, *ABCfbD—aedFEc* and *ABCfea—DbEFcd*. In each case the two parts have a common perimeter of 12 edges in a closed path. Three edges must be slit in order to flatten out a part. Each part contains *one pair* of opposite faces.

Another type of basic dissection, *ABFcab—deCfDE*, gives two symmetrical, but noncongruent, parts each containing *two pairs* of opposite faces. The common perimeter is 16 edges long.

Comment on Q434

Q434. Does there exist a real number A such that $\lim_{x\to\infty}(\sqrt{x^2+x+1}-Ax)$ exists?

If so, what is the limit?

[*Submitted by E. M. Pass*]

Comment by C. Robert Clements, The Choate School, Connecticut.

The following is another, perhaps more elementary, solution to *Q*434. We write

$$\lim_{x\to\infty}(\sqrt{x^2+x+1}-Ax) = \lim_{x\to\infty}\left(\frac{x^2+x+1-A^2x^2}{\sqrt{x^2+x+1}+Ax}\right)$$

$$= \lim_{x\to\infty}\left[\frac{x+1+1/x-A^2x}{\sqrt{1+\frac{1}{x}+\frac{1}{x^2}}+A}\right].$$

Clearly for $A=1$ the limit is $1/(\sqrt{1}+1)=1/2$.

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.

Q444. Suppose that n teams in a league play one game between each pair during the season and the final results show a "perfect" lineup, i.e., the first place team won all games, the second place team won all but one, etc., while the last place team lost them all. Prove or disprove that the ith place team lost against all jth place teams for $i>j$.

[*Submitted by Frank Dapkus*]

Q445. Show that $6k(2k-1)+1$ can never be expressed as the cube of an integer if $k\neq 0,\ 1/2$.

[*Submitted by R. S. Luthar*]

Q446. Show that the units digit of the sum of the distinct digits in any system of numeration with an odd base is zero. With an even base the units digit of the digit sum is one-half the base.

[*Submitted by Charles W. Trigg*]

Q447. Verify that $0.6666\cdots+(0.6666\cdots)^2=1.1111\cdots$

[*Submitted by Harold B. Curtis*]

Q448. Let $a_n>0$ and suppose $\sum_{n=1}^{\infty} a_n<\infty$. If $f(x)$ is positive and nonincreasing for $0<x\leqq A=\sum_{n=1}^{\infty} a_n$ and $\int_0^A f(x)dx<\infty$, then $\sum_{n=1}^{\infty} a_n f(r_n)<\infty$ where $r_n=\sum_{m=n}^{\infty} a_m$.

[*Submitted by Simeon Reich, Israel*]

(Answers on page 11.)

ACKNOWLEDGMENT

The Editorial Board acknowledges with thanks the services of the following mathematicians, not members of the Board, who have kindly assisted by evaluating papers submitted for publication in the MATHEMATICS MAGAZINE.

H. L. Alder, C. B. Allendoerfer, R. V. Anderson, A. R. Ansari, L. W. Beinke, G. A. Bergum, N. Boukidis, E. E. Burniston, J. B. Carrell, R. E. Chandler, D. G. Chapman, H. S. M. Coxeter, A. Z. Czarnecki, J. M. A. Danby, F. R. DeMeyer, M. P. Drazin, L. C. Eggan, H. W. Eves, M. L. Faulkner, L. D. Geissinger, W. J. Harrington, L. H. Hook, J. M. Kingston, V. L. Klee, R. R. Korfhage, E. A. Maier, J. A. Marlin, J. R. Rabung, J. Riordan, J. L. Selfridge, I. J. Silfies, R. D. Stalley, R. A. Struble, and A. Walvekar.

have not compressed it yet). This number is doubled again for S_2 and so on. S is now not rectifiable, although the tangent still turns continuously.

References

1. The thirteen books of Euclid's elements, trans. by Sir Thomas L. Heath, Cambridge, 1926.

2. The works of Archimedes, ed. by T. L. Heath, Cambridge, 1897. (on spirals.)

3. Observations sur la composition des mouvements, Roberval, Mémoires de l'Académie Royale des Sciences, 6 (1730).

4. G. T. Whyburn, What is a curve?, Amer. Math. Monthly, 49 (1942) 493–497.

5. H. A. Thurston, On the definition of a tangent-line, Amer. Math. Monthly, 71 (1964).

6. G. H. Hardy, A Course of Pure Mathematics, Cambridge University Press, 1908.

7. A. J. Ward, On Jordan curves possessing a tangent everywhere, Fund. Math., 28 (1937) 280–288.

8. G. Valiron, Sur les courbes qui admettent une tangente en chaque point, Ann. of Math., 2 (1927) 46–51.

9. T. M. Flett, The definition of a tangent to a curve, Edinburgh Math. Notes, 41 (1957) 1–9.

ANSWERS

A444. Let $T_1 \cdots T_n$ be the lineup (T_1 is the first place team). T_2 could have lost only against T_1, since T_1 won all games and T_2 needs one loss. T_3 obviously lost against T_1 (the all out winner) and against T_2, which needs only one loss and already has one. Continuing this reasoning to T_n proves the theorem in the affirmative.

A445. $6k(2k-1)+1=y^3$ implies that $8k^3=y^3+(2k-1)^3$. This is possible only if $k=1/2$ or zero which contradicts the hypothesis.

A446. In a system of numeration with base r, the sum of the distinct digits $0+1+2+\cdots+(r-1)$ is $r(r-1)/2$, a triangular number. If the base is odd, $r(r-1)/2$ is an integer so the sum is a multiple of r. If the base is even, the sum is $(\overline{r-1}+0)/2$. Since $r-1$ is odd the units digit of the sum is $10/2$ or one-half the base of numeration.

A447. The equation may be written as $2/3+(2/3)^2=6/9+4/9=10/9$ or or $1.1111\cdots$

A448. We have $a_n=r_n-r_{n+1}$. Also $f(r_n)\leqq f(x)$ for all x in $[r_{n+1}, r_n]$. It follows that

$$a_nf(r_n) \leqq \int_{r_{n+1}}^{r_n} f(x)dx.$$

That is

$$\sum_{n=1}^{N} a_nf(r_n) \leqq \int_{r_{N+1}}^{r_1} f(x)dx \int_0^A f(x)dx$$

for $r_{N+1}>0$.

Noting that $a_nf(r_n)>0$, the result follows.

(Quickies on page 52.)

Analytic Geometry

HARRY LEVY and LUCRETIA LEVY, University of Illinois

This textbook for the basic analytic geometry course stresses the relationship of analytic geometry to other, modern mathematical topics—sets, functions, linear algebra, and vectors—and involves the student early and actively in the development of the theory. Central to the authors' development of each topic is the inclusion of extensive exercises and problem sets which reinforce inductively the student's understanding of the major formulas and theorems of analytic geometry. 480 pages, $7.95 (probable). Publication: May 1969

Elements of Trigonometry

TULLIO J. PIGNANI
and PAUL W. HAGGARD, East Carolina University

Suitable for use in a terminal mathematics course or as a preparation for further mathematical study, this textbook offers students a current and thorough introduction to the basic elements of trigonometry. The authors present trigonometric functions clearly and precisely, with definitions, theorems, and proofs set off from the main body of the text and illustrated by worked examples. Wherever possible, computations have been simplified, primarily through the use of three-place tables. Solutions Manual available. 284 pages. $7.50

Arithmetic: SKILLS AND PROBLEM SOLVING

DONALD CONWAY and MARTIN J. DREYFUSS,
San Jose City College

A clear, well-balanced treatment of basic mathematics, this book is written for students who have not yet mastered essential arithmetic skills. It aims to give them a firm grasp of basic concepts and procedures—addition, multiplication, subtraction, and division—and a proficiency in problem solving. Numerous practical applications are included in the text, and each chapter contains a large number of drills and verbal problem sets, all carefully graded for difficulty. In addition, there are review problems at the end of each major section of the book. Answer Key available. 453 pages. $8.50