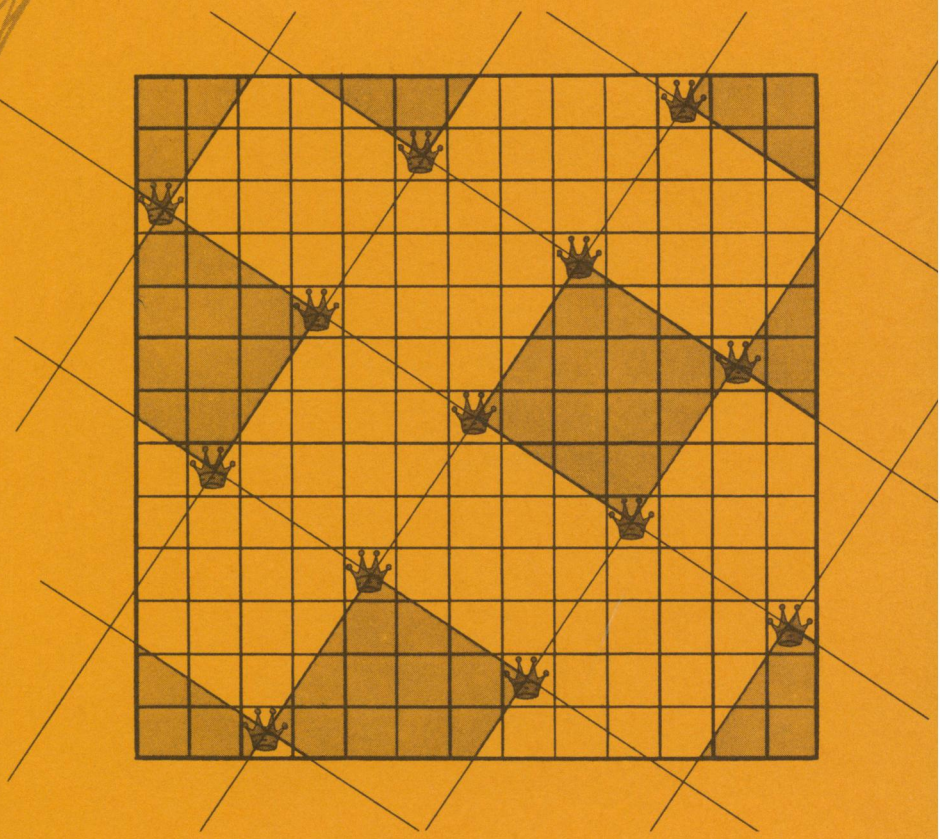
MATHEMATICS MAGAZINE



Vol. 50, No. 2
March, 1977
CODEN: MAMGA8

CHESSBOARD PRIMES • FINITE GEOMETRIES
WANKEL GEOMETRY • COUNTERFEIT COINS

New texts & new editions for '77

COLLEGE ALGEBRA

J.S. Ratti, University of South Florida

This *new* text contains a clear and logical presentation of the topics typically covered in a college algebra course. It is written in a relaxed, conversational style and is neither too theoretical nor too elementary for the average student. Basic computational skills are stressed and a straightforward, uncomplicated approach is maintained throughout.

1977 About 384 pages

COLLEGE ALGEBRA AND TRIGONOMETRY

William G. Ambrose, West Texas State University

Here is a *new* text that stresses problem-solving as the means to obtaining a sound understanding of the topics traditionally treated in a college algebra and trigonometry course. The author's approach is an excellent blend of modern and traditional treatments. *(Solutions Manual, gratis.)*

1977 About 560 pages

ESSENTIALS OF TRIGONOMETRY, Second Edition

Irving Drooyan, Walter Hadel and **Charles C. Carico,** all, Los Angeles Pierce College

The *second edition* of this successful text continues to provide a clear, well-balanced treatment of standard trigonometric topics. A heavy emphasis is placed on the properties of trigonometric functions, which are introduced through the use of geometric notions. Every exercise—*over 1885 in all*—has been reviewed and many have been revised. *(Instructor's Manual, gratis.)*

1977 338 pages

FINITE MATHEMATICS AND CALCULUS: Applications in Business and the Social and Life Sciences

Hugh G. Campbell and **Robert E. Spencer,** both, Virginia Polytechnic Institute and State University

The fundamentals of finite math and calculus are combined in this clearly written, well-organized new volume designed for students in business, social science, and life science programs. A heavy emphasis is placed on motivating the student and over 120 optional applications are provided, many of which are presented graphically for added appeal.*(Solutions Manual, gratis.)*

1977 About 640 pages

ELEMENTARY LINEAR ALGEBRA Second Edition

Bernard Kolman, Drexel University

Now in a *new* edition, this leading text continues to provide a clear and gradual introduction to postulational and axiomatic mathematics for students who have completed a calculus course. *This edition features:* increased coverage of geometric material: tighter organization: many more illustrative examples, exercises, and figures. *(Solutions Manual, gratis.)*

1977 About 312 pages

A SURVEY OF MODERN ALGEBRA, Fourth Edition

Garrett Birkhoff, Harvard University, and **Saunders MacLane,** University of Chicago

The updated *fourth edition* of this classic text introduces your students to the most important ideas of modern algebra. It is also suitable for a terminal course in algebra because it systematically treats those topics that are most important for applications. An introduction is given to Boolean algebra.

1977 About 488 pages

PROBABILITY AND STATISTICAL INFERENCE

Robert V. Hogg, University of Iowa, and **Elliot A. Tanis,** Hope College

The fundamental concepts of mathematical statistics and probability receive a clear and logical treatment in this outstanding *new* text written for the first post-calculus course in statistics. An abundance of timely, relevant problems are scattered throughout.

1977 About 416 pages

MATHEMATICS APPLIED TO CONTINUUM MECHANICS

Lee A. Segel, Weizmann Institute of Science and Rensselaer Polytechnic Institute; with material on elasticity by G. H. Handelman, Rensselaer Polytechnic Institute.

This outstanding *new* text and reference volume uses mathematics to analyze continuum models of fluid flow and solid state deformation. It is designed for advanced undergraduate and graduate level students in applied mathematics, physical science, and engineering programs.

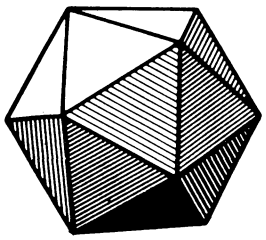
1977 About 640 pages

Macmillan Publishing Co., Inc. 100A Brown Street, Riverside, New Jersey 08075

Macmillan

MATHEMATICS MAGAZINE

Volume 50, Number 2, March 1977



COVER: Arrangements of non-attacking queens on a chessboard provide insight into the interface between geometry and algebra. The specific pattern illustrated here can be used (see page 69) to give an unusual proof of a classic theorem concerning prime numbers.

ARTICLES

69 A Theorem about Primes Proved on a Chessboard, *by Loren C. Larson.*

75 Extrema of Polynomials, *by Ralph P. Boas, Jr., and Murray S. Klamkin.*

79 Some Finite Point Geometries, *by Jane W. Di Paola.*

NOTES

84 Powers mod *n*, *by Charles Small.*

87 Rotary Engine Geometry, *by David H. Nash.*

90 Counterfeit Coin Problems, *by Bennet Manvel.*

92 Geoboard Triangles with One Interior Point, *by Charles S. Weaver.*

94 Ode to the Continuum Hypothesis, *by Maurice Machover.*

95 The Number of Square Matrices of a Fixed Rank, *by Lawrence Verner.*

96 Diamond Inequalities, *by Murray S. Klamkin and Ernest C. Schlesinger.*

PROBLEMS

99 Proposals

100 Solutions

NEWS AND LETTERS

105 Comments on recent issues; answers and hints for the 1976 Putnam examination; announcement of the 1977 Chauvenet Prize.

EDITORIAL POLICY

Mathematics Magazine is a journal of collegiate mathematics designed to enrich undergraduate study of the mathematical sciences. The *Magazine* should be an inviting, informal journal emphasizing good mathematical exposition of interest to undergraduate students. Manuscripts accepted for publication in the *Magazine* should be written in a clear and lively expository style. The *Magazine* is not a research journal, so papers written in the terse "theorem-proof-corollary-remark" style will ordinarily be unsuitable for publication. Articles printed in the *Magazine* should be of a quality and level that makes it realistic for teachers to use them to supplement their regular courses. The editors especially invite manuscripts that provide insight into applications and history of mathematics. We welcome other informal contributions, for example, brief notes, mathematical games, graphics and humor.

Editorial correspondence should be sent to: Mathematics Magazine, Department of Mathematics, St. Olaf College, Northfield, Minnesota 55057. Manuscripts should be prepared in a style consistent with the format of Mathematics Magazine. They should be typewritten and double spaced on $8\frac{1}{2}$ by 11 paper. Authors should submit the original and one copy and keep one copy as protection against possible loss. Illustrations should be carefully prepared on separate sheets of paper in black ink, the original without lettering and two copies with lettering added; the printers will insert printed letters on the illustration in the appropriate locations.

Authors planning to submit manuscripts may find it helpful to obtain the more detailed statement of guidelines available from the editorial office.

ABOUT OUR AUTHORS

Loren C. Larson ("A Theorem about Primes Proved on a Chessboard") has been on the mathematics faculty at St. Olaf College since 1968 when he completed his Ph.D. in algebra (non-standard ring theory) at the University of Kansas. This article is the result of his development of an idea suggested in one of Polya's little known contributions to recreational mathematics found, of all places, in the John White collection of chess books at the Cleveland Public Library.

Ralph Boas and Murray Klamkin ("Extrema of Polynomials") are both well known to readers of *Mathematics Magazine.* Boas is currently editor of the *Monthly* and is a past president of the Mathematical Association of America. Klamkin, inveterate problem proposer and solver, has recently returned to academia after working at the Ford Motor Company for many years. Boas once used the problem of the maximal box cut from a square piece of paper as an example of a calculus max-min problem that nobody can guess the answer to, and Klamkin countered by showing how to do the problem without calculus. Ensuing exchanges resulted in their article in this issue.

Jane Di Paola ("Some Finite Point Geometries") completed her Ph.D. at CUNY in 1967 after pauses in her education caused by World War II (flutter analysis in aircraft) and family (three children). She has now "retired" to Florida Atlantic University where she is an adjunct professor of mathematics and an active publisher of research in geometry. This article grew out of a presentation to the Hilbert Mathematics Society of NYU of a lecture "which would be understood by undergraduates and also be directly connected with my own research."

BUSINESS INFORMATION. Mathematics Magazine is published by the Mathematical Association of America at Washington, D.C., five times a year in January, March, May, September, and November. Ordinary subscriptions are $12 per year. Members of the Mathematical Association of America or of Mu Alpha Theta may subscribe at special reduced rates. Colleges and university mathematics departments may purchase bulk subscriptions (5 or more copies to a single address) for distribution to undergraduate students.

Subscription correspondence and notice of change of address should be sent to A. B. Willcox, Executive Director, Mathematical Association of America, Suite 310, 1225 Connecticut Avenue, N.W., Washington, D.C. 20036. Back issues may be purchased, when in print, from P. and H. Bliss Co., Middletown, CT 06457.

Advertising correspondence should be addressed to Raoul Hailpern, Mathematical Association of America, SUNY at Buffalo, Buffalo, New York 14214.

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

A Theorem about Primes Proved on a Chessboard

An elementary treatment of a class of solutions to the n-queens problem leads to a proof of Fermat's theorem on primes which are sums of two squares.

LOREN C. LARSON
St. Olaf College

Arrange queens on a 13×13 chessboard according to the following rule: place a queen on the center square and from it locate others by making successive (2, 3) movements — two squares to the right and three squares upward (top and bottom edges are identified, as well as right and left). The resulting queen placement (FIGURE 1) shows exactly one queen in each row and column, and no two on the same diagonal; as such, it is a solution to the n-queens problem (to place n nonattacking queens on the $n \times n$ chessboard) for $n = 13$. The solution is distinguished from other solutions in two respects: (i) it is **regular,** meaning that the queens are located at successive (s, t) movements from each other, for some integers s and t (a more precise definition will be given later), and (ii) it is **doubly symmetric,** meaning that it is invariant under a 90° rotation of the board about the center square.

More generally, suppose that u and v are positive integers and $u^2 + v^2$ is an odd prime p. We will show that queens located at successive (u, v) movements from a queen on the center square of the $p \times p$ chessboard give a regular, doubly symmetric solution to the p-queens problem. Conversely, we will see that regular, doubly symmetric solutions to the p-queens problem, for p a prime, yield positive integers u and v such that $u^2 + v^2 = p$. In the final section we will show by a simple combinatorial argument that there is a regular, doubly symmetric solution to the p-queens problem whenever p is a prime of the form $4k + 1$. Combining this result with the preceding implication gives a proof of Fermat's Two-Square Theorem: *primes of the form* $4k + 1$ *can be expressed as the sum of two squares.*

This proof of Fermat's theorem is both elementary and concrete. It avoids the usual first step of knowing that -1 is a quadratic residue modulo p when p is a prime of the form $4k + 1$. Moreover it uses the chessboard to provide a specific geometrical setting for illustrating and interpreting abstract concepts usually first encountered in an introductory abstract algebra course. The ideas on which this approach is based are scattered throughout references [1] and [2]. The chief insight — relating Fermat's Two-Square Theorem to the n-queens problem — is due to George Polya.

Preliminaries

The additive group of integers will be denoted by Z, and $\bar{Z}_n = \{1, 2, 3, \ldots, n\}$ will denote the cyclic group of order n, having the operation of addition modulo n. If x is an integer, $[x]$ will denote that integer between 1 and n inclusive which is congruent to x modulo n. (Since we will be working on an $n \times n$ chessboard, there will be no need to write $[x]_n$ to indicate the modulus.) There is little danger of confusion in using $[x]$ to denote an element of Z and also an element of $\bar{Z}_n$, for the context will make the intention clear.

For convenience we will identify the chessboard with the group $\bar{Z}_n \times \bar{Z}_n$. Geometrically, the group element (i, j) represents the square in the ith column (from the left) and the jth row (from the bottom). A **regular solution** to the n-queens problem is a solution in which the queens are located on the squares (represented by the elements) of the coset $(a, b) + \langle (s, t) \rangle$ for some $(a, b), (s, t) \in \bar{Z}_n \times \bar{Z}_n$, where $\langle (s, t) \rangle$ is the cyclic subgroup of $\bar{Z}_n \times \bar{Z}_n$ generated by (s, t). In this case, we will say that $(a, b) + \langle (s, t) \rangle$ is a regular solution.

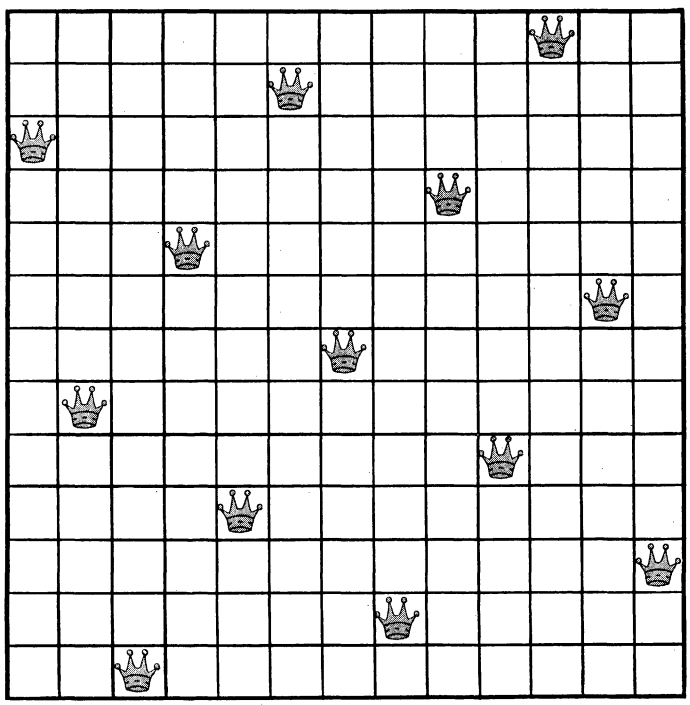


FIGURE 1

It is important to observe that every regular solution can be expressed in the form $(n, c) + \langle (1, d) \rangle$ for some $c, d \in \bar{Z}_n$. For, suppose that $(a, b) + \langle (s, t) \rangle$ is a regular solution. We know that $k(s, t)$ is a generator of $\langle (s, t) \rangle$ whenever k is an integer relatively prime to n. (Geometrically, the solution can be generated by many different regular movements.) Since s must be relatively prime to n in order that each column be occupied (similarly for t and the rows), there exists an integer r, relatively prime to n, such that $rs \equiv 1 \pmod{n}$. For this r, $r(s, t)$ is of the form $(1, d)$ for some $d \in \bar{Z}_n$. Thus $\langle (s, t) \rangle = \langle r(s, t) \rangle = \langle (1, d) \rangle$. Since a queen occurs in column n, we have, for some $c \in \bar{Z}_n$, $(n, c) \in (a, b) + \langle (s, t) \rangle$, or equivalently, $(n, c) \in (a, b) + \langle (1, d) \rangle$. It follows, then, that $(a, b) + \langle (s, t) \rangle = (n, c) + \langle (1, d) \rangle$. (For the example in the introduction, $c = 3$ and $d = 8$.)

We are interested in finding conditions on c and d so that $(n, c) + \langle(1, d)\rangle$ will be a solution to the n-queens problem. It is easy to see that a necessary condition is that d be relatively prime to n (so that each row be occupied); but this is not sufficient, since, for example, $d = 1$ violates the diagonal requirements. Notice that two queens lie on the same rising diagonal (diagonals having slope 1) if the differences (in Z) of their coordinates are the same, and on the same falling diagonal if the sums (in Z) of their coordinates are equal. For the coset above, queens are located on the squares $(i, [c + id])$ for $i = 1, 2, \ldots, n$. Since $i + [c + id] \equiv c + i(d + 1) \pmod{n}$, the sums of these coordinates will be different provided that $d + 1$ is relatively prime to n. Similarly, since $[c + id] - i \equiv c + i(d - 1) \pmod{n}$, the differences will be distinct if $d - 1$ is relatively prime to n. Thus, a sufficient condition for $(n, c) + \langle(1, d)\rangle$ to be a solution is that $d - 1$, d and $d + 1$ each be relatively prime to n. We leave it as an exercise to prove that this condition is also necessary. (Warning: this converse is not immediate since two of the coordinate sums (differences) may be equal in $\bar{Z}_n$, but unequal in Z.) We summarize the preceding discussion in the following formal lemma:

FUNDAMENTAL LEMMA. *The placement $(n, c) + \langle(1, d)\rangle$ is a solution to the n-queens problem if and only if $d - 1$, d and $d + 1$ are each relatively prime to n.*

An immediate corollary helps explain why the 8-queeens problem is so much more difficult than the 7-queens problem, which most beginners solve very quickly. We will state and prove it here, even though we will not need it (nor, for that matter, the "only if" part of the Fundamental Lemma) for the main result of the paper.

COROLLARY. *There exists a regular solution to the n-queens problem if and only if $n \equiv \pm 1 \pmod{6}$.*

Proof. We have seen that regular solutions have the form $(n, c) + \langle(1, d)\rangle$ for some c and d. If $n \equiv \pm 1 \pmod{6}$ we get a regular solution by taking $d = 2$ (ordinary knight moves). However, for $n \equiv 0, 2, 3, 4 \pmod{6}$ we cannot have regular solutions since one of $d - 1$, d, $d + 1$ is divisible by 3 and at least one of them is even.

From Number Theory to the Chessboard

Suppose that p is an odd prime number and that u and v are positive integers such that $u^2 + v^2 = p$. Choose an integer r so that $r(u, v) = (1, d)$ for some $d \in \bar{Z}_p$. Then $r^2u^2 + r^2v^2 = r^2p$, $1^2 + d^2 \equiv 0 \pmod{p}$ and therefore $d^2 \equiv -1 \pmod{p}$. Thus $(d + 1)(d - 1) \equiv d^2 - 1 \equiv -2 \pmod{p}$. It follows that $d - 1$, d and $d + 1$ are each relatively prime to p and therefore $(1, d)$ movements will generate a regular solution. The center square has coordinates $((p + 1)/2, (p + 1)/2)$, so in order that $(p, c) + \langle(1, d)\rangle$ have a queen on the center square, it is necessary and sufficient that

$$c + \left(\frac{p+1}{2}\right) d \equiv \frac{p+1}{2} \pmod{p}$$

or

$$2c + d \equiv 1 \pmod{p}. \tag{1}$$

Suppose that c is so determined. Now under a 90° clockwise rotation, the queen located on the square $(i, [c + id])$ will rotate to the square $([c + id], [1 - i])$. But this square is occupied by a queen in $(p, c) + \langle(1, d)\rangle$, since $[c + [c + id]d] = [c + cd + id^2] = [c(1 + d) - i] = [(1 - d)/2)(1 + d) - i] = [(1 - d^2)/2) - i] = [1 - i]$. Therefore the solution is doubly symmetric.

From the Chessboard to Number Theory

Suppose now that p is a prime and that $(p, c) + \langle(1, d)\rangle$ is a regular, doubly symmetric solution to the p-queens problem. Since the 2×2 board does not admit such a solution, the prime p is odd. Observe that a queen is located on the center square, since queens off the center come in sets of four,

these located at quarter turns from each other (rotational symmetry). (Incidentally, this shows that p has the form $4k + 1$.)

From among all the queens on the board, pick one that is closest to the queen on the center square; suppose it is located at a (u, v) movement from the center square. Because of rotational symmetry we may suppose that u and v are positive. (Other closest queens will be located at $(v, -u)$, $(-u, -v)$, and $(-v, u)$ movements from the center square.) Because the solution is regular, no two queens can be located closer together than these two queens. (To get from one queen to another requires an $i(1, d) \in \bar{Z}_p \times \bar{Z}_p$ movement for some integer i, and this same movement could be made from the center square.)

The center queen and the two queens located at (u, v) and $(v, -u)$ movements from it, occupy three vertices of a square region; the fourth vertex of this square is occupied by a queen in the solution since it is a $(u, v) + (v, -u) \in \bar{Z}_p \times \bar{Z}_p$ movement from the center (and each summand is a multiple of a $(1, d)$ movement). Furthermore, no queen in the solution will be located in the interior of this square (since that would violate our choice of u and v). In the same way, every queen on the board can be associated with a square region whose vertices are given by its own position and those queens at $(u, v), (v, -u)$ and $(u, v) + (v, -u)$ movements from it. It is understood that left and right, top and bottom edges are identified, so that squares which overlap an edge are continued on the opposite side (see FIGURE 2). In this way the $p \times p$ chessboard is dissected into p regions (one for each queen) each of equal area. Since the total area of the chessboard is p^2, each individual square has an area equal to p. It follows that the side length of each square is $\sqrt{p}$, and therefore, from the Pythagorean theorem, that $p = u^2 + v^2$.

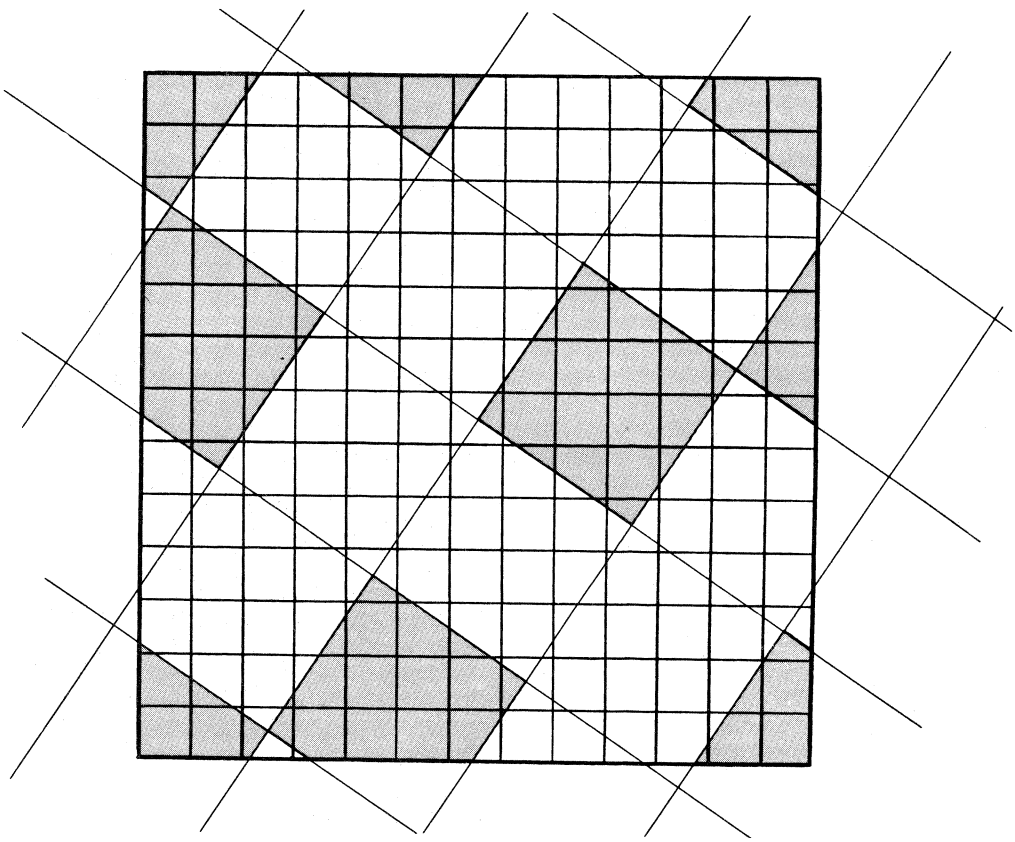


FIGURE 2

It may be instructive to point out that the queen positions in a regular solution are part of a lattice that extends to the entire plane. This can be seen algebraically by first observing that the mapping ϕ: $Z \times Z \to \bar{Z}_n \times \bar{Z}_n$ defined by $((x, y))\phi = ([x], [y])$ is a group homomorphism. Let H be the cyclic subgroup of $Z \times Z$ generated by (u, v). Then the elements of $(H\phi)\phi^{-1}$ may be interpreted geometrically as the positions of the queens obtained by tiling the entire plane with copies of the chessboard having queens located on the squares $H\phi$. However, $(H\phi)\phi^{-1}$ is a subgroup of $Z \times Z$, and therefore it is a lattice of dimension two, having a fundamental region of area equal to the absolute value of the determinant of the matrix gotten by expressing the lattice basis in terms of the canonical basis of $Z \times Z$. Now an arbitrary regular solution to the n-queens problem is a translation of $H\phi$ for some cyclic group H of $Z \times Z$, and this corresponds to the same translation in $Z \times Z$ of the subgroup $(H\phi)\phi^{-1}$.

Fermat's Two Square Theorem

In order to prove Fermat's result, we need to show that there is a regular, doubly symmetric solution to the p-queens problem whenever p is a prime of the form $4k + 1$. To do this, we will count the total number of regular solutions for the $p \times p$ board in two different ways.

LEMMA. *The number of regular solutions to the p-queens problem, where p is a prime, is* $p(p - 3)$.

Proof. We know that regular solutions have the form $(p, c) + \langle(1, d)\rangle$. Clearly we do not get a solution when d is $p, p - 1$, or 1. But any of the other $p - 3$ possibilities for d, in $\bar{Z}_p$, will produce regular solutions, since in these cases $d - 1$, d, and $d + 1$ will each be relatively prime to p. Since c can take on any of p values, the total number of regular solutions is $p(p - 3)$.

A second way of counting the regular solutions is to partition them into three classes, depending upon their symmetry — doubly symmetric, symmetric (invariant under a 180° rotation but not a 90° rotation), or nonsymmetric (no symmetry). The symmetries of the square consist of four reflections and four rotations, and these form a group G, under composition. If x denotes a regular solution and $U \in G$, the regular solution which results from x by applying the transformation U will be denoted by xU. Two regular solutions x and y are **essentially the same** if and only if there exists a $U \in G$ such that $xU = y$. This is an equivalence relation on the set of all regular solutions. The equivalence class of a solution x consists of all those solutions that can be obtained from x by rotation and reflection. For each regular solution x, let H_x denote the set of all symmetries of x; that is, $H_x = \{U \in G \mid xU = x\}$. H_x is a subgroup of G. Furthermore, if $U, V \in G$, $xU = xV$ if and only if $xUV^{-1} = x$, and this happens if and only if $UV^{-1} \in H_x$. It follows that the number of elements in the equivalence class of x is equal to the index of H_x in G, and this is 2, 4, or 8 depending upon whether x is doubly symmetric, symmetric, or nonsymmetric respectively. Thus we have the following lemma:

LEMMA. *The number of regular solutions to the n-queens problem is* $2x + 4y + 8z$, *where x, y, z are, respectively, the number of essentially different doubly symmetric, symmetric, and nonsymmetric regular solutions to the n-queens problem.*

Now suppose that p is a prime of the form $4k + 1$. Combining the results of the preceding two lemmas, we know that $p(p - 3) = 2x + 4y + 8z$. Since, in this equation, $p \equiv 1 \pmod 4$, it becomes $2 \equiv 2x \pmod 4$. But this completes the proof, since this last equation implies that x, the number of essentially different regular, doubly symmetric solutions, is not zero.

Finally, we can show that the positive integers u and v in Fermat's result are unique. To do this, it is sufficient to prove that there are only two regular, doubly symmetric solutions to the p-queens problem — a single solution, and its horizontal reflection, both of which induce the same positive integers u and v for which $u^2 + v^2 = p$. So, suppose that $(p, c) + \langle(1, d)\rangle$ is a regular, doubly symmetric solution to the p-queens problem. Since a queen is located on the square $(1, [c + d])$, there must also be (by rotational symmetry) a queen on the square $([c + d], p)$. This means that

(2) $$c + [c + d]d \equiv p \pmod{p}.$$

The fact that the center square is occupied means that (1) holds, so that we may substitute $c \equiv (1 - d)/2$ from (1) into (2) to get

$$\left(\frac{1-d}{2}\right) + \left(\frac{1+d}{2}\right) d \equiv p \pmod{p}$$

which simplifies to

(3) $$d^2 + 1 \equiv 0 \pmod{p}.$$

Thus d satisfies $x^2 + 1 = 0$ over the field $\bar{Z}_p$. Alternatively, if we substitute $d \equiv 1 - 2c$ from (1) into (2) we see that c must satisfy $x^2 + (x - 1)^2 = 0$ over $\bar{Z}_p$. Thus the existence of a regular, doubly symmetric solution to the p queens problem, for p a prime of the form $4k + 1$, also implies the existence of two solutions to each of the equations $x^2 + 1 = 0$ and $x^2 + (x - 1)^2 = 0$ in $\bar{Z}_p$. Since $\bar{Z}_p$ is a field, these second order polynomial equations can have only two solutions in $\bar{Z}_p$, which implies that there can be only two possible values for d and c. But once one of these values is known, so is the other by equation (1), proving that there are at most two regular, doubly symmetric solutions to the p-queens problem when p is a prime.

In conclusion, we note that these latter equations offer an alternative, albeit less elegant, procedure for proving the existence of a regular, doubly symmetric solution to the p-queens problem for p a prime of the form $4k + 1$; simply choose d by (3) and c by (1) and apply the argument following equation (1).

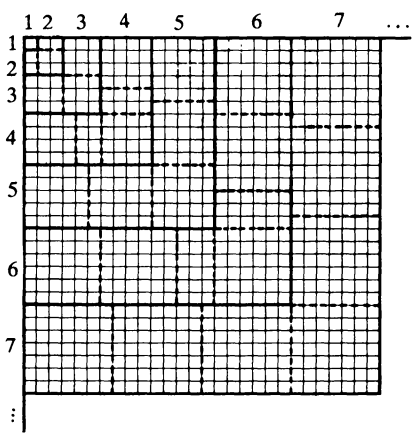
References

[1] Maurice Kraitchik, La Mathématique des Jeux ou Récréations Mathématiques, Chapter XIII, Le Problème des Reines, Bruxelles, 1930, pp. 300–356.

[2] G. Polya, Über die "doppelt-periodischen" Lösungen des n-Damen Problems, Mathematische Unterhaltungen und Spiele, Dr. W. Ahrens. Zweiter Band, B. G. Teubner, Leipzig, 1918, pp. 363–374.

Proof without words: Cubes and squares

$$1^3 + 2^3 + 3^3 + \cdots + n^3$$
$$= (1 + 2 + 3 + \cdots + n)^2$$



— J. Barry Love
National Liberty Corp.
Valley Forge, Penn.

Extrema of Polynomials

Summa contra calculus: algebraic alternatives to derivative methods of polynomial optimization.

Ralph P. Boas, Jr.
Northwestern University

Murray S. Klamkin
University of Alberta

A well-known elementary calculus problem is to maximize the volume of an open box that can be made from a rectangular sheet $2a \times 2b$ by cutting congruent squares (with side x) out of the four corners and folding up. Here, $V = 4x(a - x)(b - x)$ is to be maximized for $0 < x < a$. Although the solution by calculus is both easy and effective, we shall give an alternate solution by a judicious application of the inequality between the arithmetic and geometric means. This method is less direct than the application of calculus, but it has the advantage that it can be used in precalculus courses (even in secondary schools) to solve optimization problems of polynomial type. In particular, all the standard problems about optimal tin cans, boxes, etc., can be analysed by our alternate method. This is possible because the equation $dV/dx = 0$ comes out of the arithmetic-geometric mean inequality with neither any appeal to limiting processes nor computation of the derivative as such.

The inequality between the arithmetic and geometric means, which can be proved in quite an elementary way [**1**, **2**], says that if $y_1, y_2, \ldots, y_n$ are non-negative numbers, then

$$\frac{1}{n}(y_1 + y_2 + \cdots + y_n) \geqq (y_1 \cdot y_2 \cdots y_n)^{1/n}, \tag{1}$$

with equality holding if and only if all the y_i are equal. (Here and throughout, the index i takes the values $1, 2, \ldots, n$.) It follows at once that *if the y_i are constrained to satisfy $\Sigma y_i = k$ (a constant) then the product Πy_i is maximized for $y_i = k/n$ and the maximum is $(k/n)^n$.*

In our example of the open box, the volume we wish to maximize is a multiple of a product of terms whose sum is constant. Specifically, $V = 2 \cdot 2x(a - x)(b - x)$ where the sum $2x + (a - x) + (b - x)$ is constant. But we cannot in this case guarantee that all three terms are equal, i.e., that $2x = a - x = b - x$, as would be required in order to apply the condition stated above. However, we can equally well maximize any constant multiple of V, so we will seek a suitable multiple.

To do this we allocate the unknown multiple of V among the three terms in such a way as to make the multiples of the terms x, $a - x$, and $b - x$ equal to each other. In other words, we try to find positive numbers p, q, and r such that $px = q(a - x) = r(b - x)$ while $px + q(a - x) + r(b - x)$ is still constant. Then $pqrV = 4pxq(a - x)r(b - x)$ would be the desired multiple of V.

To insure that the sum $k = px + q(a - x) + r(b - x)$ is constant we need require only that $p = q + r$. Then the equality of the three terms $(q + r)x$, $q(a - x)$, and $r(b - x)$ can be insured if and only if $x = qa/(2q + r) = rb/(2r + q)$. This condition reduces to a quadratic equation for $s = q/r$, one (and only one) of whose roots is positive. After finding it, we can use the optimization condition stated above to express the maximum value of V in terms of the original parameters a and b:

$$V_{\max} = \frac{4}{pqr}\left(\frac{k}{3}\right)^3 = \frac{4(qa + rb)^3}{27(q + r)qr} = \frac{4(sa + b)^3}{27s(s + 1)}.$$

The connection of this solution with the calculus condition $dV/dx = 0$ requires further explanation. If we let λ denote the common value of the terms px, $q(a-x)$ and $r(b-x)$, then $p = \lambda/x$, $q = \lambda/(a-x)$, and $r = \lambda/(b-x)$. Substitution of these expressions in the relation $p = q + r$ leads to

$$\frac{1}{x} - \frac{1}{a-x} - \frac{1}{b-x} = 0,$$

which is equivalent to $(\log V(x))' = V'(x)/V(x) = 0$.

We now extend the method so that it can be used to find the maxima of

$$|P(x)| = \prod_{i=1}^{n} |x - r_i|^{n_i}, \qquad r_i < r_{i+1},$$

in an interval $r_j < x < r_{j+1}$, where the n_i are positive integers. We consider, instead of $|P(x)|$, the modified product

$$Q(x) = \Pi\{w_i(x - r_i)\}^{n_i},$$

where the weights w_i are real and satisfy $w_i(x - r_i) > 0$ for $r_j < x < r_{j+1}$, and $\Sigma n_i w_i = 0$. Let $N = \Sigma n_i$. Then the inequality (1) between the arithmetic and geometric means, applied to the N positive numbers $w_i(x_i - r_i)$, each repeated n_i times, tells us that $Q(x)$ is maximized, for $r_j < x < r_{j+1}$, when all the $w_i(x - r_i)$ are equal. If we let λ stand for the common value of $w_i(x - r_i)$ then $w_i = \lambda/(x - r_i)$; hence the requirement $\Sigma n_i w_i = 0$ can be expressed as

$$\Sigma \frac{n_i}{x - r_i} = 0, \qquad r_j < x < r_{j+1}, \tag{2}$$

which is a necessary and sufficient condition for x to maximize $Q(x)$. Consequently $\max|P(x)|$, $r_j < x < r_{j+1}$, has the value $\Pi|r - r_i|^{n_i}$, where r is the (only) root of (2) in $r_j < x < r_{j+1}$.

Logarithmic differentiation reveals that (2) is just $P'(x)/P(x) = 0$. To complete our argument we should derive this fact by elementary means (i.e., without calculus), for then we would have a purely algebraic demonstration that $P(x)$ is maximized at one of the zeros of $P'(x)$. Moreover, since (2) is expressed in terms of the roots r_i of $P(x)$, to obtain a root of (2) directly we would first have to find all roots of $P(x)$. Knowing that the roots of (2) are just the roots of $P'(x) = 0$ would avoid this laborious task.

So, to conclude our program, we should show that if

$$P(x) = \prod_{i=1}^{n} (x - r_i)^{n_i} = x^m + a_1 x^{m-1} + a_2 x^{m-2} + \cdots + a_m,$$

then

$$P(x) \sum_{i=1}^{n} \frac{n_i}{x - r_i} = mx^{m-1} + (m-1)a_1 x^{m-2} + (m-2)a_2 x^{m-3} + \cdots + a_{m-1}.$$

This can be done in a straightforward but unimaginative way by induction on the number of roots of $P(x)$. We will obtain it below by an entirely different method.

We should note, before doing this, that the method just described is not completely new. Applications of the arithmetic-geometric means inequality to extremum problems have appeared previously many times, e.g., see [**3**, **4**, **5**]. Garver [**4**] uses a procedure similar to that used here but only illustrates the method on a number of specific examples containing two or three variables (and reducible to two). Also, he does not obtain the derivative equation which allows one to proceed directly to the desired critical values.

Lennes [**6**] gives a different algebraic procedure (well known to algebraic geometers) but he illustrates it only for polynomials of degrees 2, 3 and 4. He obtains the local extrema of $P(x)$ (if any) by

determining the conditions under which $P(x) = b$ has a double root. This root is then obtained by elimination. In Lennes' method, the roots of $P(x)$ need not all be real. (Incidentally, our method can also be extended for complex roots, with more bother, by using complex conjugate weights for complex conjugate roots.) We will extend Lennes' method to a general polynomial

$$P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n = 0$$

since it helps complete the program begun above and leads to some nice applications of determinants.

Let b be a number such that $P(x) = b$ has a double root, let $-r, -r, -r_1, -r_2, \ldots, -r_{n-2}$ denote the roots of $P(x) = b$, and define S_i by

$$\prod_{i=1}^{n-2} (x + r_i) \equiv x^{n-2} + S_1x^{n-3} + S_2x^{n-4} + \cdots + S_{n-2}.$$

Then, by multiplying both sides of this equation by $(x + r)^2$ and equating coefficients, we obtain $n - 1$ linear equations in the $n - 2$ unknowns $S_1, S_2, \ldots, S_{n-2}$:

$$\begin{aligned}
2r + S_1 &= a_1, \\
r^2 + 2rS_1 + S_2 &= a_2, \\
r^2S_1 + 2rS_2 + S_3 &= a_3, \\
&\vdots \\
r^2S_{n-4} + 2rS_{n-3} + S_{n-2} &= a_{n-2}, \\
r^2S_{n-3} + 2rS_{n-2} &= a_{n-1}.
\end{aligned} \tag{3}$$

This system is consistent if and only if one of the equations is a linear combination of the others, and this occurs precisely when

$$\begin{vmatrix}
a_1 - 2r & 1 & 0 & 0 & \cdots & 0 \\
a_2 - r^2 & 2r & 1 & 0 & \cdots & 0 \\
a_3 & r^2 & 2r & 1 & \cdots & 0 \\
a_4 & 0 & r^2 & 2r & \cdots & 0 \\
\vdots & \vdots & & & & \vdots \\
a_{n-1} & 0 & 0 & 0 & \cdots & 2r
\end{vmatrix} = 0.$$

Expanding along the first column, we can express this equation as

$$(a_1 - 2r)D_{n-2} - (a_2 - r^2)D_{n-3} + a_3D_{n-4} - a_4D_{n-5} + \cdots = 0,$$

where D_n denotes the following tridiagonal determinant of nth order:

$$\begin{vmatrix}
2r & 1 & 0 & \cdots & 0 \\
r^2 & 2r & 1 & \cdots & 0 \\
0 & r^2 & 2r & & \\
\vdots & \vdots & \vdots & & \vdots \\
0 & 0 & 0 & \cdots & 2r
\end{vmatrix}$$

Now it follows by induction that $D_n = (n + 1)r^n (n \geqq 2)$; this expression reduces the determinantal equation to the expected derivative equation:

$$nr^{n-1} - a_1(n - 1)r^{n-2} + a_2(n - 2)r^{n-3} + \cdots = 0.$$

(The coefficient signs alternate since the root is $-r$ rather than r.) This shows, by elementary means, that the extrema of $P(x)$ occur at the zeros of $P'(x)$.

Lennes' method can also be applied to find the critical points of rational functions $P(x)/Q(x)$. Without loss of generality, we can take $P(x)$ to be of nth degree and $Q(x)$ of degree $\leqq n-1$. (Note that if deg $Q >$ deg P we would consider instead Q/P, while if deg $Q =$ deg P, then $P/Q = k + R/Q$ where deg $R <$ deg Q.) If

$$P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n \quad \text{and} \quad Q(x) = b_1x^{n-1} + b_2x^{n-2} + \cdots + b_n,$$

then for $P(x) = bQ(x)$ to have a double root we obtain equations (3) with a_i replaced by $a_i + bb_i$. Solving these as before, we obtain what corresponds to $P'(x) - bQ'(x) = 0$. Since $P(x) = bQ(x)$ this is equivalent to

$$\frac{P'(x)}{P(x)} - \frac{Q'(x)}{Q(x)} = \frac{d}{dx} \log \frac{P(x)}{Q(x)} = 0.$$

Prior to Lennes, Genese [7] used a similar idea that is easier to carry out. To use Genese's method, we must find a b such that

$$U \equiv x^m + a_1x^{m-1} + a_2x^{m-2} + \cdots + a_m - b$$

should have $(x-r)^2$ as a factor. For U to be divisible by $x-r$, we must have, by the remainder theorem, that $b = r^m + a_1r^{m-1} + \cdots + a_m$. Then $U = x^m - r^m + a_1(x^{m-1} - r^{m-1}) + \cdots$, from which, by rearranging the terms, we get

$$\frac{U}{x-r} = x^{m-1} + (r + a_1)x^{m-2} + (r^2 + a_1r + a_2)x^{m-3} + \cdots . \tag{4}$$

If $U/(x-r)$ is again divisible by $(x-r)$, we must get zero if we set $x = r$ on the right hand side of equation (4):

$$r^{m-1} + (r + a_1)r^{m-2} + (r^2 + a_1r + a_2)r^{m-3} + \cdots = 0.$$

This is nothing but the ubiquitous derivative equation with its terms somewhat rearranged. Regrouping yields the familiar form:

$$mr^{m-1} + (m-1)a_1r^{m-2} + (m-2)a_2r^{m-3} + \cdots + a_{m-1} = 0.$$

Note that if U is also divisible by a higher power of $x-r$, say $(x-r)^e$ where e is the maximum exponent, then if e is odd, U does not have a maximum or minimum value at $x = r$.

These three algebraic methods provide noncalculus alternatives for polynomial optimization. In each case the extreme points of $P(x)$ are recognized by a special property — equality in the arithmetic-geometric mean relation, double roots of the equation $P(x) = b$, or repeated factors of $P(x)$ — that do not require the concept of the derivative. But, as must be, the result in each case is precisely the derivative equation $P'(x) = 0$.

References

[1] G. H. Hardy, J. E. Littlewood, G. Pólya, Inequalities, Cambridge University Press, Cambridge, 1934, p. 20 (iii).

[2] Problem 807, this MAGAZINE, 45 (1972) 172.

[3] E. F. Beckenbach, R. Bellman, An Introduction to Inequalities, Random House, New York, 1961.

[4] R. Garver, The solutions of problems in maxima and minima by algebra, Amer. Math. Monthly, 42 (1935) 435.

[5] N. D. Kazarinoff, Geometric Inequalities, Random House, New York, 1961.

[6] N. J. Lennes, Note on maxima and minima by algebra methods, Amer. Math. Monthly, 17 (1910) 9.

[7] R. W. Genese, Mess. Math., 1 (1872) 32–34.

[8] T. J. Fletcher, Doing without calculus, Math. Gazette, 55 (1971) 4–17.

Some Finite Point Geometries

Finite sets with distinguished subsets called lines give examples of the theory of balanced incomplete block designs.

JANE W. DI PAOLA
Florida Atlantic University

This article provides an introduction to small planes, an area of finite mathematics which is the subject of active current research. Since small affine and projective planes have appeared many times in the undergraduate literature, less emphasis is placed upon them here than might be expected. However, small Bolyai-Lobechevskian planes are presented with considerable detail. We will conclude our brief survey by introducing balanced incomplete block designs as a generalization of finite planes. A suggested reading list (in order of difficulty) provides guidance for those interested in further study.

One's earliest experience with school geometry concerns the relation between points and lines: two distinct points 'determine' a line and if two distinct lines meet they have exactly one point in common. From school gometry we are also familiar with the idea that in the same plane two lines sometimes meet and sometimes do not meet. In the latter case the lines are called parallel. After placing these notions in a more formal setting, we shall look at some finite sets of points within which we can distinguish certain subsets to be called 'lines' which, together with the points, will behave in the way we should expect points and lines to behave.

We begin by introducing a set of postulates for a plane, or more technically, for a **planar incidence geometry.** Consider a set $\mathcal{V}$ of points and a set $\mathcal{L}$ of certain distinguished subsets of $\mathcal{V}$, called lines. A point p is said to be **incident** with line L if and only if p is a point of L. If p is incident with L we say p **is contained in** L, or, p is on L or L **is on** p. A system $(\mathcal{V}, \mathcal{L})$ is said to be a **plane** if it satisfies the following postulates:

(i) A line is a set of points containing at least two points.

(ii) Two distinct points are contained in one and only one line.

(iii) There exists a line and a point not on the line.

(iv) If a subsystem $(\mathcal{V}', \mathcal{L}')$ contains a line L, a point p not on L, and all the points on every line determined by any pair of points in $\mathcal{V}'$, then $(\mathcal{V}', \mathcal{L}') = (\mathcal{V}, \mathcal{L})$.

An example of a plane with 4 points and 4 lines is shown in FIGURE 1. The example in FIGURE 2 with 4 points and 6 lines is not a plane (according to the definition we have adopted here) since it violates postulate (iv). In general, postulate (iv) rules out any figure of more than 3 points in which each line has exactly two points and every pair of points determines a line. Such figures are called complete

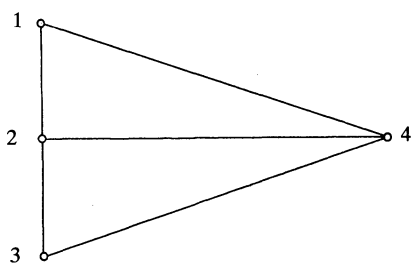


FIGURE 1

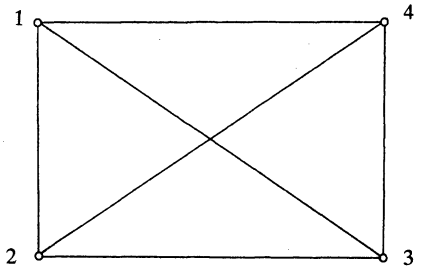


FIGURE 2

graphs on n points. (We consider the complete graph on 3 points to be trivial although it does satisfy the axioms.)

Two lines will be called **parallel** if they have no point in common. If we consider a line L and a point p not on L, the existence of which is promised in postulate (iii), there are three possibilities with respect to the number of lines on p not meeting L. These three possibilities give us the following alternative parallel postulates:

1. *Projective parallel postulate*: Given a line L and a point p not on L, there is no line on p not intersecting L.
2. *Euclidean parallel postulate*: Given a line L and a point p not on L, there is exactly one line on p not intersecting L.
3. *Bolyai-Lobachevskian parallel postulate*: Given a line L and a point p not on L, there are at least two lines on p not intersecting L.

We say a plane is **projective, affine,** or **Bolyai-Lobachevskian** according to whether it satisfies the projective, Euclidean, or Bolyai-Lobachevskian parallel postulate.

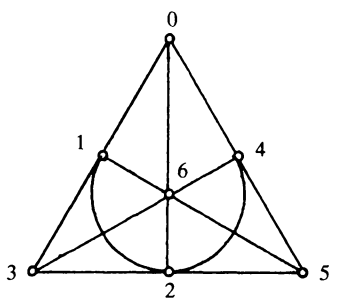


FIGURE 3

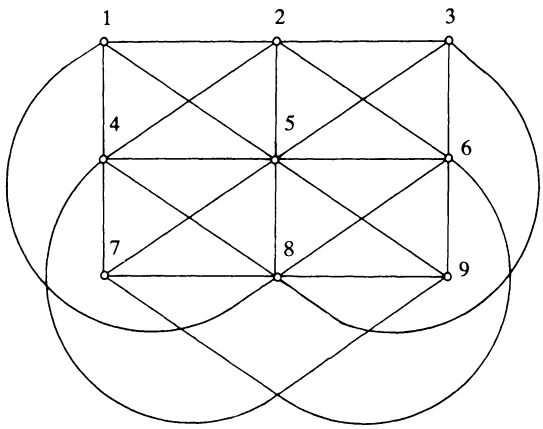


FIGURE 4

The smallest non-trivial example of a projective plane is given by the famous configuration of Fano (FIGURE 3) with seven points ($\mathcal{V} = \{0,1,2,3,4,5,6\}$) and seven lines of 3 points each:

0	1	3		2	3	5		4	5	0		6	0	2
1	2	4		3	4	6		5	6	1				

(For simplicity, we denote the line $\{0,1,3\}$, for example, by the triple 0 1 3.) The smallest non-trivial example of an affine plane (FIGURE 4) has nine points ($\mathcal{V} = \{1,2,3,4,5,6,7,8,9\}$) and twelve lines:

1	2	3		1	4	7		1	5	9		3	5	7
4	5	6		2	5	8		2	6	7		1	6	8
7	8	9		3	6	9		3	4	8		2	4	9

The smallest non-trivial examples of a finite Bolyai-Lobachevskian plane have 13 points $0, 1, 2, \ldots, 12$ and 26 lines. Here is one possible set of lines:

0	1	4		7	8	11		0	2	8		7	9	2
1	2	5		8	9	12		1	3	9		8	10	3
2	3	6		9	10	0		2	4	10		9	11	4
3	4	7		10	11	1		3	5	11		10	12	5
4	5	8		11	12	2		4	6	12		11	0	6
5	6	9		12	0	3		5	7	0		12	1	7
6	7	10						6	8	1				

We leave it as an exercise to verify that each of the models above does, in fact, satisfy the axioms and the appropriate parallel postulate.

Now that we have seen by explicit example that we can construct a finite model for each parallel postulate, we might well ask whether we can construct a mixed model. By this we mean a model in which some line-point pairs satisfy one parallel postulate and some line-point pairs satisfy another. The answer is no, at least not if we wish our model to have the property that all lines contain the same number of points. This idea is embodied in what is called the Principle of Homogeneity of planar incidence geometries: *If a planar incidence geometry has the same number of points on each line, then for each pair L, p where L is a line and p is a point not on L, the number of lines on p which do not intersect L is a constant.*

The proof of this principle is extraordinarily simple. Assume that there are k points on each line and let p be a point in $\mathcal{V}$. Since two points determine a unique line, the set of lines on p partitions the set $\{\mathcal{V} - p\}$ into disjoint subsets (each of which contains $k-1$ points). Therefore the number of lines on p is $(v-1)/(k-1)$, where v represents the number of points in $\mathcal{V}$. If L is a line not on p, then the number of lines on p that meet L is precisely k — the number of points of L. Hence the number of lines on p that do not meet L is $[(v-1)/(k-1)]-k$, independent of the choice of p or L.

The models of the projective plane and of the affine plane having three points on each line are well known and are discussed in many elementary books on geometry. These two models are each unique up to isomorphism. (An isomorphism between two incidence models is, roughly, a pointwise mapping which preserves collinearity.) The Bolyai-Lobachevskian plane with 13 points and 26 lines is not unique: there is another $B-L$ plane not isomorphic to the one given above but also having 13 points (see Hall [3], also Ryser [4]). We have only to take the lines (0 1 4), (9 10 0), (10 11 1), and (9 11 4) of the given plane, which we call G_1, and replace them by the lines (11 1 4), (9 10 11), (10 0 1), and (9 0 4) to obtain the new $B-L$ plane on 13 points, which we shall call G_2. The question now is how we know that G_2 is not isomorphic to G_1. That is indeed a difficult question, but if we examine the four line replacements carefully we can develop a method to prove non-isomorphism. We begin with some important definitions.

Two pairs of points AB and CD of a finite plane are **projective doubles** if the line determined by A and B meets the line determined by C and D and if one of the following then holds: either the line determined by A and D meets the line determined by B and C or the line determined by A and C meets the line determined by B and D. We call the intersection points of the lines determined by a set of projective doubles **associate vertices.** Two pairs of points which form a projective double satisfy one of the configurations in FIGURE 5. In either case we say X and Y are associate vertices, or simply, X is an **associate** of Y.

The configuration shown in FIGURE 5 is a familiar diagram in modern geometry. One of the basic axioms of projective geometry — the very axiom which we have called "the projective parallel

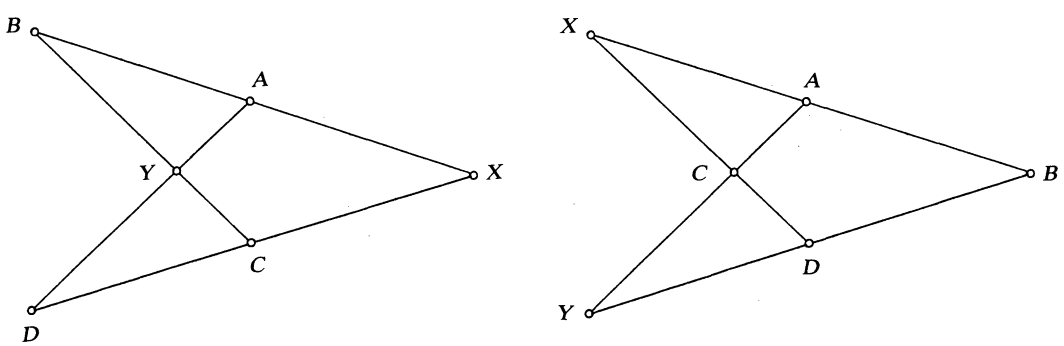


FIGURE 5

postulate" — is usually stated (see Veblen and Young [9]) as follows: If AB meets CD then AC meets BD. (Here AB means the unique line determined by the two points A and B.) It is for this reason that we call FIGURE 5 the "projective double configuration." This configuration has been used frequently to count nonisomorphic incidence systems. We shall use it to show that the two Bolyai-Lobachevskian planes on 13 points do not have the same structure and so are not isomorphic.

In order to characterize each of the $B - L$ planes on 13 points we list the associates of each vertex. We can do this as a routine clerical job. For example, in G_1, we determine the associates of the point O by noting that the pencil of lines on O consists of six lines: (0 1 4), (0 3 12), (0 9 10), (0 5 7), (0 11 6), (0 2 8). By examining the 15 combinations of the six pairs (1, 4), (3, 12), (9, 10), (5, 7), (11, 6), (2, 8), we find the following intersections [(a, b) denotes the line determined by a and b]:

$$(3,4) \cap (1,12) = 7 \qquad (3,10) \cap (8,12) = 8$$

$$(1,10) \cap (4,9) = 11 \qquad (3,6) \cap (11,12) = 2$$

$$(1,2) \cap (4,8) = 5 \qquad (5,9) \cap (7,10) = 6$$

Thus the vertex (point) O has six associate vertices namely, 7, 11, 5, 8, 2, 6. We do this for each vertex in G_1 and for each vertex in G_2. In G_1 each vertex has six associates and in G_2 no vertex has six associates. This means that G_1 and G_2 do not have the same structure, i.e., they are not isomorphic. In G_2 some vertices have 3 associates and some have 4 associates. Further study of the projective doubles and their associate vertices reveals other interesting properties of the two planes on 13 points. These discoveries we leave to the reader.

In the two $B - L$ planes which we have considered the number of parallels to a given line through a point not on it is three, whereas the classical approach to the non-Euclidean geometry of Bolyai and Lobachevsky assumes that the number of parallels to a given line through a point not on it is two. We might wonder therefore whether there exists a finite $B - L$ plane with the same number of points on each line in which the number of parallels to a given line through a point not on it is two? The answer is easily shown to be no. We use the following notation. Let b represent the number of lines in the plane, r the number of lines on each point, k the number of points on each line and v the number of points in the plane. By counting in two ways the number of line-point incidences we obtain $vr = bk$. Since each pair of points appears in exactly one line, the number r of lines on a given point is $(v-1)/(k-1)$; thus we also have the relationship $r(k-1) = v - 1$. The number of parallels to a given line through a point not on it is $r - k$. If we eliminate v and let $r - k = 2$, we obtain $bk = k^3 + 3k^2 + k - 2$, or, since $k \neq 0$, $b = k^2 + 3k + 1 - 2/k$. Since b is an integer this implies either $k = 1$ or $k = 2$. Postulate (i) rules out $k = 1$ and postulate (iv) rules out $k = 2$.

(It may be worth noting that the value $k = 2$ yields the complete graph on n points and this would be an $(n-1)$-dimensional projective space with 2 points on each line. The force of postulate (iv) is to rule out as planes those configurations which can better be thought of as higher dimensional spaces. For example, if we take $k = 2$ and $v = 4$, the configuration is the complete graph on 4 vertices which can be thought of as a tetrahedron. This constitutes a 3-dimensional projective space with two points on each line and 3 points in each plane.)

Finite planes are a subset of a class of finite incidence structures called **balanced incomplete block designs.** Each such design consists of a set of v points arranged into b blocks of k points each in such a way that each point appears r times and each pair of points appears together in a block exactly λ times. The integers v, b, r, k, λ are called the parameters of the design. The same counting argument used in proving the Principle of Homogeneity (there $\lambda = 1$) shows that the parameters of a balanced incomplete block design satisfy the relations: $vr = bk$ and $r(k-1) = \lambda(v-1)$.

A projective plane of order n has parameters $v, b, r, k, \lambda = n^2 + n + 1, n^2 + n + 1, n + 1, n + 1, 1$ and an affine plane of order n has parameters $n^2, n^2 + n, n + 1, n, 1$. From an affine plane of order n we may construct a projective plane of order n and the process is reversible. Finite projective and affine planes are known to exist for $n = p^t$ where p is a prime number. Whether there are such planes

of other orders is in general an unsolved problem although some conditions are known which rule out infinite sets of numbers as candidates for n. The smallest unsolved case is $n = 10$ and a great deal of current research centers upon the search for a projective plane of order 10.

It is easy to show (see **[10]** p. 97) that a balanced incomplete block design with parameters r, k, λ such that $k + 1 < r \leqq 2k$, $k \geqq 3$, $\lambda = 1$ is a model of a Bolyai-Lobachevskian plane. Since there are many designs with such parameters there are many $B - L$ planes. However, there are historical motives for restricting our attention to $B - L$ planes which have the same number of parallels as non-parallels with respect to a given line and a point not on the line, that is, those with $r - k = k$. Under this condition, in addition to the two models already discussed with $k = 3$, only two others are known, one with 4 points on a line and one with 5 points on a line. The known $B - L$ plane with 5 points on a line is easily written out by taking 5-subsets of a set of 41 points in two classes represented by

$$(x + 1,\ x + 37,\ x + 16,\ x + 18,\ x + 10) \quad \text{and} \quad (x + 8,\ x + 9,\ x + 5,\ x + 21,\ x + 39).$$

We let x assume each value in the set $0, 1, 2, \ldots, 40$ and use addition modulo 41 to obtain 82 lines. We leave the reader with an unsolved problem: Can you find some simple operation on this plane, perhaps somehow analogous to the projective double configuration, which will yield a new plane with 5 points on each line?

Reading List

[1] L. R. Lieber, The Education of T. C. Mits, New York, 1942.
Chapter XV gives a brief and lucid introduction to finite Euclidean (affine) geometry. It would be a mistake, however, not to read the entire book.

[2] W. Prenowitz and M. Jordan, Basic Concepts of Geometry, Waltham, Mass., 1965.
This is a readable college text. Chapter 8 contains a number of models of the theory of incidence and these are presented in a manner suitable for individual study. The book also gives an extremely clear introduction to non-Euclidean geometry.

[3] M. Hall, Jr., A survey of combinatorial analysis, in I. Kaplansky, E. Hewitt, M. Hall, Jr., and R. Fortet, Some Aspects of Analysis and Probability, New York, 1958.
Although now outdated by the recent progress made in combinatorics in the past decade, this article is an easy introduction to block designs.

[4] H. J. Ryser, Combinatorial Mathematics, New York, 1965.
One of the Carus Monographs of the Mathematical Association of America, this is a clearly written exposition of combinatorics by one of the leading contributors to research in this explosive area of modern mathematics.

[5] L. M. Graves, A finite Bolyai-Lobachevskian plane, Amer. Math. Monthly, 69 (1962) 130–132.
This short piece might have been sub-titled "a mathematician long distinguished in analysis discovers the existence of finite geometry." It was the starting point of a series of investigations by others into the existence of models of Bolyai-Lobachevskian geometry.

[6] T. G. Ostrom, Ovals and finite Bolyai-Lobachevsky planes, Amer. Math. Monthly, 69 (1962) 899–901.
This is a follow-up to Graves' article listed above. The postulates we have given here for $B - L$ planes are in the form used by Ostrom.

[7] J. W. Di Paola, Configurations in small hyperbolic planes, Ann. New York Acad. Sci., Art. 1 (1970) 93–103.
The reader will find herein more details of the structure of the models of $B - L$ planes together with some applications to game theory.

[8] R. C. Bose, On the construction of balanced incomplete block designs, Ann. Eugenics, 9 (1939) 353–399.
This is the classic basic reference in the construction of block designs.

[9] O. Veblen and J. W. Young, Projective Geometry, New York, 1910.
This two volume work was the definitive text on incidence geometry for more than half a century. It is still worth reading and its many exercises are worth doing.

[10] P. Dembowski, Finite Geometries, New York, 1970.
This is the current bible for geometry scholars. It is difficult because of its comprehensiveness. It is a 'must' for graduate students and something which even the casual reader should know exists.

NOTES

Powers mod n

CHARLES SMALL
Queen's University

Arithmetic mod n is a rich source of elementary examples of more general algebraic phenomena. In this note we illustrate that theme by considering three related questions mod n:

1. For odd primes p it is well known that -1 is a square mod p if and only if $p \equiv 1 \bmod 4$. This result, which plays an important role in elementary number theory (see [4], Chapter V) suggests the more general question: Given integers $k > 1$ and $n > 1$, when is it true that -1 is a kth power mod n?
2. We can always write -1 as a sum of $n-1$ squares mod n: $-1 = 1^2 + 1^2 + \cdots + 1^2$. But usually -1 is a sum of fewer than $n-1$ squares mod n; in fact we will see that $n-1$ squares are required only if $n \leqq 4$. How many squares do we need to represent -1 mod n, as a function of n?
3. Given n, can we find $k > 1$ such that every integer is a kth power mod n? If so, what is the smallest such k?

Naturally, there are a great many other interesting questions of this type. For example, the question of when -1 is a power of 2 mod n is investigated in [6], the general question of representing integers efficiently as sums of kth powers mod n is considered in [7], and an analogue of Goldbach's problem (on representing numbers as sums of primes) is treated in [1].

The following three theorems completely answer the questions raised above:

THEOREM 1. *Write* $n = 2^f p_1^{e_1} \cdots p_s^{e_s}$ *where* $f \geqq 0$, *the* p_i *are distinct odd primes, the* e_i *are* $\geqq 1$, *and* $s \geqq 0$, *and write* $k = 2^a l$, $a \geqq 0$, l *odd. Then* -1 *is a* k*th power* mod n *if and only if one of the following holds*:

(a) $a = 0$ (i.e., k *is odd*),

(b) $a \geqq 1$ (i.e., k *is even*), $f = 0$ *or* $f = 1$ (i.e., $4 \nmid n$), *and for each* i $(1 \leqq i \leqq s)$, $p_i \equiv 1 \bmod 2^{a+1}$.

THEOREM 2. *For each* n, *let* $s(n)$ *denote the smallest integer* r *such that* -1 *is a sum of* r *squares* mod n. *Then*:

$$s(n) = 1 \quad \text{if} \quad 4 \nmid n \quad \text{and} \quad p \nmid n \quad \text{for all primes} \quad p \equiv 3 \bmod 4;$$

$$s(n) = 2 \quad \text{if} \quad 4 \nmid n \quad \text{and} \quad p \mid n \quad \text{for some prime} \quad p \equiv 3 \bmod 4;$$

$$s(n) = 3 \quad \text{if} \quad 4 \mid n \quad \text{but} \quad 8 \nmid n; \quad \text{and} \quad s(n) = 4 \quad \text{if} \quad 8 \mid n.$$

The number $s(n)$ computed in Theorem 2 is the analogue, for $Z/(n)$, of the *Stufe* ("level") of a non-formally-real field. (A field F is **formally real** if 0 is not a sum of non-zero squares in F, or equivalently, if -1 is not a sum of squares in F.) If F is *not* formally real, the smallest r such that -1 is a sum of r squares in F is called the ***Stufe*** ("level") of F. It is well known (see [5], Chapter 2) that this number is always a power of 2, and that conversely fields of *Stufe* 2^n exist for all $n \geqq 0$.

THEOREM 3. *For each integer* $n > 1$ *let* $h(n)$ *denote the smallest integer* $k > 1$ *with the property that every element of* $Z/(n)$ *is a* k*th power*; *put* $h(n) = \infty$ *if no such* k *exists. Then* $h(n)$ *is finite if and only if* n *is squarefree. When* n *is squarefree, write* n *as a product of distinct primes,* $n = p_1 p_2 \cdots p_s$; *then* $h(n)$ *is the smallest prime* q *which does not divide* $(p_1 - 1)(p_2 - 1) \cdots (p_s - 1)$.

The question answered by Theorem 3 is first raised, as far as I know, at the end of [3], in which the following related problem is solved: given n, can we find $k > 1$ such that the congruence $x^k \equiv x \bmod n$ holds for all x? If so, what is the smallest such k?

The proofs we shall give for these three results all follow the same pattern: first use the Chinese Remainder Theorem ([4], Theorems 20 and 22) to reduce to the case where n is a prime power p^e; then argue directly, isolating the case $p = 2$ if necessary, and using the fact ([4], Theorems 23 and 28) that when p is an odd prime the group of units mod p^e is, for any $e \geq 1$, cyclic of order $p^e - p^{e-1}$. (The reader may wish to try using these hints to prove the theorems himself before reading further!)

Proof of Theorem 1. By the Chinese Remainder Theorem, the factorization $n = 2^f p_1^{e_1} \cdots p_s^{e_s}$ yields a corresponding decomposition $Z/(n) \cong Z/(2^f) \times Z/(p_1^{e_1}) \times \cdots \times Z/(p_s^{e_s})$. It is clear from this that -1 is a kth power mod n if, and only if, -1 is a kth power mod 2^f and mod $p_i^{e_i}$ for each i, $1 \leq i \leq s$. Hence the result follows from the following two lemmas:

LEMMA 1. *Let k be even and $f \geq 1$. Then -1 is a kth power* mod 2^f *if and only if $f = 1$.*

LEMMA 2. *Let p be an odd prime and write $k = 2^a l$, $a \geq 0$, l odd. Then for any $e \geq 1$ the following are equivalent*:

(i) -1 *is a* 2^a*th power* mod p^e,

(ii) -1 *is a kth power* mod p^e,

(iii) $p \equiv 1 \bmod 2^{a+1}$.

In Lemma 1, the "if" is trivial. Conversely, if -1 is a kth power mod 2^f with $f > 1$, the facts that $Z/(2^f)$ maps homomorphically onto $Z/(4)$ and that k is even would allow us to conclude that -1 is a square mod 4; but this is false.

To prove Lemma 2, we can first of all assume $a \geq 1$ (i.e., k is even), for both Lemma 2 and Theorem 1 are trivial when $a = 0$ (i.e., k is odd). Now, to complete the proof, we show (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): Since l is odd, $x^{2^a} \equiv -1 \bmod p^e$ implies $x^k = (x^{2^a})^l \equiv -1 \bmod p^e$.

(ii) $\Rightarrow$ (iii): If $x^k \equiv -1 \bmod p^e$ then $(x^k)^2 = x^{2k} \equiv 1 \bmod p^e$, so the order of x in the group $U(p^e)$ of units mod p^e, call it t, divides $2k = 2^{a+1}l$. However t cannot divide k, for we would then have $1 \equiv x^k \equiv -1 \bmod p^e$, contradicting the fact that p is odd. But clearly $t \mid 2^{a+1}l$, $t \nmid 2^a l$ together imply $2^{a+1} \mid t$; say $t = 2^{a+1}s$. Then since x has order t, x^s is an element of order 2^{a+1}. But $U(p^e)$ is a group of order $p^e - p^{e-1}$ ([4], Theorem 23) and therefore can have an element of order 2^{a+1} only if 2^{a+1} divides $p^e - p^{e-1} = p^{e-1}(p-1)$, and clearly this is equivalent to $2^{a+1} \mid p - 1$, i.e., $p \equiv 1 \bmod 2^{a+1}$.

(iii) $\Rightarrow$ (i): If $p \equiv 1 \bmod 2^{a+1}$ then $p^e \equiv p^{e-1} \bmod 2^{a+1}$ and we can write $2^{a+1}m = p^e - p^{e-1}$ for some m. Now $U(p^e)$ is cyclic ([4], Theorem 28) so we can choose a generator σ, i.e., an element of order $p^e - p^{e-1} = 2^{a+1}m$. Then σ^m is an element of order 2^{a+1}, which implies $(\sigma^m)^{2^a} \equiv -1 \bmod p^e$. This completes the proof of Lemma 2 and thus of Theorem 1 too.

Note that it follows from Lemma 2 that if -1 is a kth power mod p^e for *some* e, then the same is true for *all* e, for condition (iii) is independent of e.

Proof of Theorem 2. The first step, as before, is to write $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where the p_i are distinct primes and $e_i \geq 1$. The Chinese Remainder Theorem tells us that $Z/(n)$ is isomorphic to the direct product of the $Z/(p_i^{e_i})$, and it is clear from this that $s(n)$ is the maximum of the $s(p_i^{e_i})$. Hence we must study $s(p^e)$ for primes p.

For the even prime, there is little to do: $s(2) = 1$, $s(4) = 3$, $s(8) = 4$, and since every positive integer is a sum of 4 squares (Lagrange's Theorem), $s(2^e) = 4$ for all $e > 3$.

For odd primes p, we have:

LEMMA 3. *Let p be an odd prime. Then $s(p^e) = 1$ for all $e \geq 1$ if $p \equiv 1 \bmod 4$, and $s(p^e) = 2$ for all $e \geq 1$ if $p \equiv 3 \bmod 4$.*

Before proving this, the reader should verify that it does complete the proof of Theorem 2.

Half of Lemma 3 has already been proved: if $p \equiv 1 \bmod 4$, it follows from Lemma 2 above that -1 is a square mod p^e, i.e., $s(p^e) = 1$, for all $e \geqq 1$. When $p \equiv 3 \bmod 4$ the same Lemma shows that $s(p^e) > 1$. However in this case we can find integers x and y, neither divisible by p, with $x^2 + y^2 \equiv -1 \bmod p$. We are using here the fact that -1 is a sum of two squares mod p. The standard proof of this can be found, for example, in [2] (Lemma 7.7), and the reader should find it easy and instructive to modify that proof to show more generally that if a, b, c are non-zero elements in a finite field F, then there exist x and y in F with $ax^2 + by^2 = c$; cf. [7], 3.2 and the remark following it.

Now, given $x^2 + y^2 \equiv -1 \bmod p$, we proceed by induction. Namely, suppose $x^2 + y^2 \equiv -1 \bmod p^m$, say $x^2 + y^2 + 1 = p^m b$, and choose c such that $2cx \equiv -b \bmod p$; this is possible because $p \nmid x$, so that $2x$ is a unit mod p. We claim that $(x + cp^m)^2 + y^2 \equiv -1 \bmod p^{m+1}$; this will clearly finish the proof. On the one hand, since $2cx + b \equiv 0 \bmod p$, we have $p^m(2cx + b) \equiv 0 \bmod p^{m+1}$. On the other hand, since $x^2 + y^2 + 1 = p^m b$ we have $(x + cp^m)^2 + y^2 + 1 \equiv x^2 + 2cxp^m + y^2 + 1 = p^m(2cx + b) \bmod p^{m+1}$. Clapping the two hands together gives the desired result.

Note that the "$s(n) = 1$" part of Theorem 2 is the case $a = 1 = l$ of Theorem 1, and that the two theorems agree on this overlap!

Proof of Theorem 3. As always, start by writing $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ where the p_i are distinct primes and the exponents e_i are positive, and observe that by the Chinese Remainder Theorem, $Z/(n)$ breaks up as the corresponding direct product $Z/(p_1^{e_1}) \times \cdots \times Z/(p_s^{e_s})$. It is clear from this that if $h(n)$ is finite, then each $h(p_i^{e_i})$ is finite. Now if p is prime and $e > 1$ and $k > 1$, p cannot be a kth power mod p^e: for if $p = x^k + mp^e$ then $p \mid x$, but then $p^2 \mid x^k + mp^e = p$, a contradiction. Hence $h(p^e) = \infty$ if $e > 1$, and consequently $h(n) = \infty$ unless n is squarefree.

Now let $n = p_1 p_2 \cdots p_s$ where the p_i are distinct primes. Let $U(n)$ (resp. $U(p_i)$) denote the group of units mod n (resp. mod p_i); fix k and define θ (resp. θ_i) to be the map $U(n) \to U(n)$ (resp. $U(p_i) \to U(p_i)$) given by $\theta(x) = x^k$ (resp. $\theta_i(x) = x^k$). Then θ is the direct product of the maps $\theta_1, \ldots, \theta_s$; in other words, the diagram

$$\begin{array}{ccc} U(n) & \simeq & U(p_1) \times \cdots \times U(p_s) \\ {\scriptstyle\theta}\downarrow & & \downarrow \\ U(n) & \simeq & U(p_1) \times \cdots \times U(p_s) \end{array}$$

commutes, where the isomorphism is the canonical one of the Chinese Remainder Theorem ([4], Theorems 20, 22) and the unlabelled map is $\theta_1 \times \cdots \times \theta_s$, i.e., $(x_1, \ldots, x_s) \mapsto (x_1^k, \ldots, x_s^k)$.

It is clear from this that $h(n)$ is the smallest $k > 1$ for which θ is onto, which is the same as the smallest $k > 1$ for which each θ_i, $1 \leqq i \leqq s$, is onto. Now it is well known that the image of θ_i has $(p_i - 1)/(k, p_i - 1)$ elements where $(k, p_i - 1)$ denotes the greatest common divisor; this is an easy consequence of the fact that $U(p_i)$ is cyclic of order $p_i - 1$. Hence θ_i is onto if and only if $(k, p_i - 1) = 1$, so that $h(n)$ is the smallest $k > 1$ such that $(k, p_1 - 1) = (k, p_2 - 1) = \cdots = (k, p_s - 1) = 1$. Clearly this is the same as the smallest prime q such that $q \nmid p_1 - 1, q \nmid p_2 - 1, \ldots, q \nmid p_s - 1$, or equivalently such that $q \nmid (p_1 - 1)(p_2 - 1) \cdots (p_s - 1)$.

Added in proof: M. J. DeLeon has pointed out to the author that Theorem 3 is proved by different methods by C. Corder in *Amer. Math. Monthly*, 23 (1976) 32–33.

References

[1] E. Cohen, A finite analogue of the Goldbach problem, Proc. A.M.S., 5 (1954) 478–483.

[2] I. Herstein, Topics in Algebra, Blaisdell, Waltham, 1964.

[3] E. Hewitt, Certain congruences that hold identically, Amer. Math. Monthly, 83 (1976) 270–271.

[4] F. Richman, Number Theory, an Introduction to Algebra, Brooks/Cole Belmont, Calif., 1971.

[5] W. Scharlau, Quadratic forms, Queen's Papers in Pure and Applied Mathematics #22, 1969.

[6] M. K. Siu, When is -1 a power of 2?, this MAGAZINE, 48 (1975) 284–286.

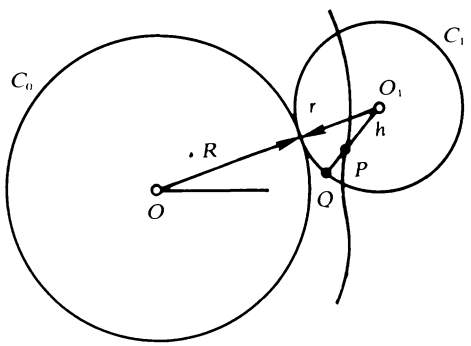
[7] C. Small, Waring's problem mod n, Amer. Math. Monthly, 84 (1977) 12–25.

Rotary Engine Geometry

David H. Nash
Research Laboratories, General Motors Corp.

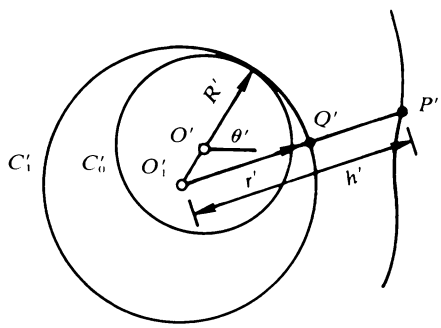
Most of the mathematics implicit in the famous rotary combustion engine of Felix Wankel predates the engine by a few centuries. We will survey in this note the classical roots of rotary engine geometry; non-mathematical background material can be found in [2]. We begin with several definitions that lead to an elegant result, known as the Bernoulli-Goldbach-Euler double generation theorem, that nicely relates the triangular rotor to its housing (bore).

Let C_0 be a circle of radius R centered at the origin O in the x-y plane. Let C_1 be a circle tangent to C_0, in the same plane, with radius r and center O_1. Let Q be a point on C_1 and P be a point different from O_1 on the straight line determined by O_1 and Q. Denote the distance from O_1 to P by h. Then the locus of P as C_1 rolls without slipping on and exterior to C_0 is called an **epitrochoid** (see FIGURE 1).



Generation of epitrochoid

FIGURE 1.



Generation of peritrochoid

FIGURE 2.

Let θ denote the angle between OO_1 and the positive x-axis measured from this axis in the counterclockwise sense and suppose P lies to the left of O_1 on the x-axis when $\theta = 0$. If (x, y) denotes the Cartesian coordinates of P, then

$$x = x(\theta) = (r + R)\cos\theta - h\cos\left(\frac{r+R}{r}\theta\right), \tag{1}$$

$$y = y(\theta) = (r + R)\sin\theta - h\sin\left(\frac{r+R}{r}\theta\right). \tag{2}$$

For convenience we write $(x, y) = E(r, R, h, \theta)$.

We next consider a similar situation in which the rolling circle is interior to the fixed circle (see FIGURE 2). To distinguish this case, we use primed notation. If $R' < r'$ and C_1' rolls without slipping on C_0' with C_0' interior to C_1', then the locus of P' is called a **peritrochoid.** If P' lies on the x'-axis to the right of O_1' when $\theta' = 0$, then

(3) $$x' = x'(\theta') = -(r' - R')\cos\theta' + h'\cos\left(\frac{r' - R'}{r'}\theta'\right),$$

(4) $$y' = y'(\theta') = -(r' - R')\sin\theta' + h'\sin\left(\frac{r' - R'}{r'}\theta'\right).$$

For convenience we write $(x', y') = \Pi(r', R', h', \theta')$.

The relations $h = r' - R'$, $r + R = h'$, $hh' = rr'$ and $h'\theta = r\theta'$ transform equations (1) and (2) into (3) and (4), and conversely. From this it follows that *every epitrochoid is a peritrochoid, and conversely.* In particular,

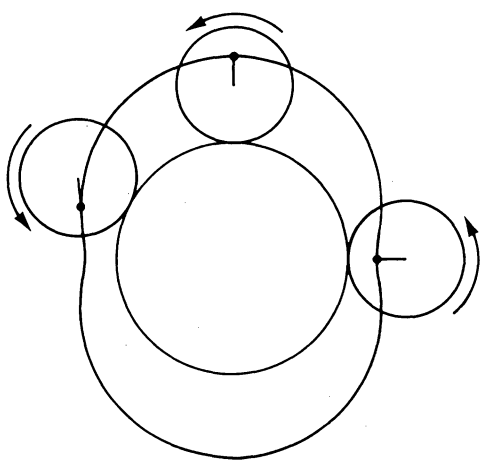
$$E(r, R, h, \theta) = \Pi\left(h\left(\frac{r+R}{r}\right), \frac{hR}{r}, r + R, \left(\frac{r+R}{r}\right)\theta\right)$$

and

$$\Pi(r', R', h', \theta') = E\left(h'\left(\frac{r'-R'}{r'}\right), \frac{h'R'}{r'}, r' - R', \left(\frac{r'-R'}{r'}\right)\theta'\right).$$

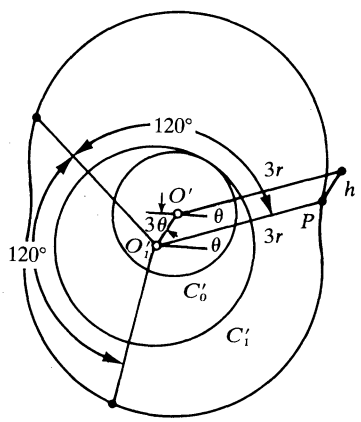
This so-called double generation theorem probably was known to the Bernoulli brothers Daniel and Nicolaus III. In 1725 the latter communicated a similar result to Goldbach, who provided a proof later that year ([**7**], p. 97; [**5**], pp. 168–170). Euler published a related paper in 1781 ([**7**], p. 97; [**4**]).

To see how the preceding relates to the rotary engine, take $R = 2r$ and $h < 3r/5$. Then $E(r, 2r, h, \theta)$ describes a two-lobed epitrochoid of the type indicated in FIGURE 3, which defines the engine bore. (In practice sealing problems cause this shape to be modified slightly ([**1**], p. 26).) By the double generation theorem, $E(r, 2r, h, \theta) = \Pi(3h, 2h, 3r, 3\theta)$. Suppose an equilateral triangular rotor with centroid O_1' has an internal gear C_1' of radius $3h$ centered at O_1', which rotates on a fixed gear C_0'



Two-lobed epitrochoid

FIGURE 3.



Rotor vertex configuration

FIGURE 4.

of radius $2h$ centered at O' (see FIGURE 4). Suppose P is a vertex of the rotor at a distance $3r$ from O_1', and O' is between P and O_1' on the x-axis when $\theta = 0$. Then the locus of P is the epitrochoid $E(r, 2r, h, \theta)$ of the bore. The condition $h < 3r/5$ ensures that C_1' always lies inside the bore, which is an obvious physical requirement. That all three rotor vertices always lie on this epitrochoid, a fact which is crucial for sealing purposes, can be verified as follows: The parametric equations for P can be expressed by

(5) $$(x, y) = -h(\cos 3\theta, \sin 3\theta) + 3r(\cos\theta, \sin\theta),$$

which represents the sum of two circular motions. The first summand corresponds to O'_1, the rotor centroid. The other rotor vertices are then given by

$$(x, y) = -h(\cos 3\theta, \sin 3\theta) + 3r(\cos(\theta + 2n\pi/3), \sin(\theta + 2n\pi/3)) \quad \text{with} \quad n = 1, 2.$$

Since $\cos 3\theta = \cos 3(\theta + 2n\pi/3)$ and $\sin 3\theta = \sin 3(\theta + 2n\pi/3)$, these vertices must lie on the epitrochoid.

In practice the axis of the crankshaft is centered at O' and torque is transmitted to the shaft via a rigidly attached eccentric which slides inside a central hole in the rotor (see [2], p. 18). Equation 5 and its interpretation show that the crankshaft completes three revolutions for each revolution of the rotor.

A number of shapes have been used for the rotor flanks, including circular arcs. It is a straightforward exercise to show that if circular arcs are used, then their radii must be at least $(9r^2 + 4h^2 - 6rh)/(3r - 4h)$ to permit rotation of the rotor in the bore. The shape that yields the theoretical maximum compression ratio — the ratio ρ of the largest to smallest volumes of the chambers formed between bore and rotor during a revolution of the rotor — is that of the inner envelope of a certain family of epitrochoids (see [1], pp. 136–139, for definitions and derivations). In practice engineering considerations force modification of this shape and depressions must be made in the flanks to facilitate combustion. It can be shown that ρ is an inreasing function of r/h ([1], p. 143), and for all bores is bounded above by $(499 + 288\sqrt{3})/13 = 76.756\ldots$. Standard rotary compression ratios are of the order of 10.

The acute angle between O'_1P and the normal to the epitrochoid of the bore at P ranges from 0 to arcsin (h/r) during a revolution of the rotor. In reality this causes a back and forth motion of the rotor apex seals (vertices) on the bore. This phenomenon causes friction and sealing problems, but is a built-in feature of the geometry.

The geometry of Wankel's rotary combustion engine is old yet elegant mathematics, now often neglected in school curricula. This article has touched only the surface of the possibilities. Related material on cycloidal curves in general can be found, e.g., in [8] and [3] and on curves of constant width in [6]. A connection between J. J. Sylvester's plagiograph and the rotary engine configuration is mentioned in [1], p. 132. A variety of rotary pumps, compressors and engines is discussed in [9].

Many references in this paper are due to the late Professor Carl B. Allendoerfer of the University of Washington, who kindly provided comments and encouragement even while he was in the hospital with a tragic illness. Discussions with Drs. Robert Davies, Sam Savage and John Steiner of General Motors Research Laboratories were informative. The referees provided several valuable suggestions. Mr. Drake Maher rendered the graphics.

References

[1] R. F. Ansdale, The Wankel RC Engine, A. S. Barnes and Co., Cranbury, N. J., 1969.
[2] D. E. Cole, The Wankel Engine, Scientific American, v. 227, Aug. 1972, 14–23.
[3] Cycloidal Curves or Tales from the Wanklenburg Woods [an Allendoerfer film, animated and in color], Coffin and Co., 619 E. Pine St., Seattle, Wash., 98122, and Modern Learning Aids, Rochester, N.Y.
[4] L. Euler, De Duplici genesi tam epicycloidum quam hypocycloidum, Acta Acad. Petrop., (1781) Pars I, (1784).
[5] P. H. Fuss, Correspondance Mathématique et Phys. de Quelques Célèbres Géomètres du XVIII Siècle, II, St. Petersburg, 1843.
[6] M. Goldberg, Rotors in polygons and polyhedra, Math. Comp., v. 14, 71 (1960) 229–239.
[7] G. Loria, Algebraische und Transzendente Ebene Kurven, Teubner, Leipzig, 1911.
[8] R. A. Proctor, A Treatise on the Cycloid and All Forms of Cycloidal Curves, Longmans, Green, London, 1878.
[9] F. Wankel, Rotary Piston Machines, London ILIFFE Books, trans. and ed. by R. F. Ansdale, 1965.

Counterfeit Coin Problems

BENNET MANVEL
Colorado State University

In January of 1945, the following problem appeared in the *American Mathematical Monthly*, contributed by E. D. Schell:

> You have eight similar coins and a beam balance. At most one coin is counterfeit and hence underweight. How can you detect whether there is an underweight coin, and if so, which one, using the balance only twice?

Since such weighing problems are today as much a part of the tradition of recreational mathematics as magic squares and mobius bands, it is interesting to note that they date only from that problem in 1945. The classic works of Loyd, Ball, Dudeney and Kraitchik contain no such problems. The responses to Schell's problem, a flurry of papers in the *Monthly*, *Scripta Mathematica*, and the *Mathematical Gazette*, contain no mention of earlier publications which might be relevant. Thus, it is apparent that this class of extremely natural and appealing puzzles is a recent invention, not an old chestnut which "crops up from time to time to puzzle and infuriate new generations of solvers" as someone wrote in 1961 (when such puzzles were just fifteen years old!).

That early spate of papers, appearing in 1945 and the next few years with a speed unheard of in these days of publication backlogs, solved, resolved, and generalized the original problem in all directions. In this paper I present several variations of the balancing problem, all of which have been solved before. The method of solution given here may be original.

We will always be dealing with a set of coins, of identical appearance, and a beam balance. We are interested in minimizing the maximum number of weighings which may be required to find the odd coin. The method of solution chosen may require solution of several types of weighing problems simultaneously, because a problem may change character after a weighing. For example, after a single use of the beam we have some coins which we know to be genuine (those on the beam, if it balances, those left off it if it does not). Thus, after one weighing we have a problem of a different type than the original one.

We shall break all of the problems dealt with into two classes: those in which the counterfeit coin is known to be underweight and those in which it is only known to be of a different weight than the genuine coins. At the very end of the paper we will examine the possibility of no counterfeit coin. For the time being, we will assume that in every case exactly one coin is not genuine. Sometimes a "standard" coin, known to be the correct weight, will be provided. We begin with the first class of problems.

THEOREM 1. *Let S be a set of coins, one lighter than the rest. The least number of weighings on a beam balance in which the light coin can be found is the unique n satisfying $3^{n-1} < |S| \leqq 3^n$.*

Proof. Suppose first that $|S| = 3^n$. Then for the first weighing, we divide S into three equal sets, S_1, S_2 and S_3, of size 3^{n-1}, and place S_1 and S_2 on opposite sides of the beam. If the scale does not balance, the light coin is on the light side of the scale; otherwise it is in S_3. In any case, we have reduced our problem to finding the light coin in a set of size 3^{n-1}. Continuing in this way, the light coin can be located after n weighings. If $|S| < 3^n$, a similar procedure can be followed, placing equal sets S_1 and S_2 of coins on the scale, leaving a set S_3 of at most 3^{n-1} coins unweighed. Again, repetitions will lead us to the light coin in at most $n-1$ more steps.

On the other hand, it is clear that a single weighing of any sort cannot do better than cut the size of the set of "suspect" coins by a factor of 3. This is so because three sets are involved in the process, two on the scale and one off, and the outcome merely distinguishes which of the three sets contains the light coin. Thus if $|S| > 3^{n-1}$, $n-1$ weighings cannot be enough to find the light coin in all cases.

We now modify the problem under consideration by assuming only that the counterfeit coin is a different weight from the others — either heavier or lighter. The general observation we need to solve this more difficult problem is the following rather strange sounding result.

LEMMA. *If in a set S of coins one coin is a different weight than the rest and each coin is labelled "possibly heavy"* (p.h.) *or "possibly light"* (p.l.), *the least number of weighings on a beam balance in which the odd coin can be found is the unique n satisfying* $3^{n-1} < |S| \leqq 3^n$.

Proof. Notice that this result is very similar to Theorem 1, in which every coin can be thought of as being labelled p.l. since the odd coin is known to be light. In fact, the weighing procedure of Theorem 1 works in this case, with one restriction. Whenever we place coins on the scale, we must be sure to put equal numbers of p.l. coins on the two sides (and therefore equal numbers of p.h. coins on the two sides, as well). If, for example, $|S| = 3^n$, we divide S into three sets of size 3^{n-1}, say S_1, S_2 and S_3, placing the same number of p.l. coins in S_1 and S_2. When S_1 and S_2 are compared on the scale, if S_1 (say) is heavier, the counterfeit coin must be among the p.h. coins in S_1 or the p.l. coins in S_2, which together constitute a set of size 3^{n-1}. If the scale balances, we are, of course, left with the set S_3, of size 3^{n-1}. Thus in every case we reduce the size of the set by a factor of 3, as in Theorem 1. For sets where $|S|$ is not a power of 3 a similar procedure is effective.

The lemma is useful because it describes a common type of weighing problem. If we know only that the counterfeit coin is an odd weight, a first weighing which does not balance leaves us with the coins on the scale each labelled "possibly heavy" or "possibly light". We are now ready to solve the problem of the odd coin in the case where a standard coin is provided.

THEOREM 2. *If we are given a set S of coins, plus a standard coin, and one coin in S is a different weight than the rest, then the least number of weighings in which the odd coin can be found is the unique n satisfying* $(3^{n-1} - 1)/2 < |S| \leqq (3^n - 1)/2$.

Proof. Let us denote by $M(n)$ the maximum number of coins for which the odd coin problem can be solved in n weighings if a standard coin is provided. The lemma claims that $M(n) = (3^n - 1)/2$. It is easy to see that this is correct for $n = 1$ and 2.

Suppose now we are given a set S of coins from which we are to find the odd coin in n weighings. On our first weighing, we must place equal sets of coins S_1 and S_2 on the scale, leaving off a set S_3. If the beam balances, we are left with S_3, so we must require $|S_3| \leqq M(n-1)$ to be able to solve the problem in that case. On the other hand, if the scale does not balance, we are left with S_1 and S_2, each coin labelled "possibly heavy" or "possibly light". So we must have $|S_1| + |S_2| \leqq 3^{n-1}$. Since the two sides of the scale must have the same number of coins, this apparently implies that $|S_1| + |S_2| = 3^{n-1} - 1$, at a maximum, but that is not so. We have a standard coin at our disposal, so we can let $|S_1| + |S_2| = 3^{n-1}$, and $|S_1| = |S_2| + 1$, using the standard coin on the S_2 side. So if the scale does not balance, we are left with 3^{n-1} coins, each labelled, a problem we know by the lemma to be solvable.

Thus we have found that we can solve the balancing problem if $|S| = (|S_1| + |S_2|) + |S_3| = 3^{n-1} + M(n-1)$. This yields $M(n) = 3^{n-1} + M(n-1)$, which leads to $M(n) = \sum_{i=0}^{n-1} 3^i$. Thus $M(n) = (3^n - 1)/2$, as the sum of a geometric series.

THEOREM 3. *Let S be a set of more than two coins, one a different weight than the others. The least number of weighings in which the odd coin can be found is the unique n satisfying* $(3^{n-1} - 3)/2 < |S| \leqq (3^n - 3)/2$.

Proof. Clearly we must begin by comparing two equal sets S_1 and S_2 on the balance, leaving off a set S_3. If the beam does not balance, the counterfeit is in $S_1 \cup S_2$, each coin is labelled "possibly heavy" or "possibly light" and so, by the lemma, $|S_1 \cup S_2| \leqq 3^{n-1}$. Since we must balance equal sets of coins and have no standard coin, the maximum for $|S_1 \cup S_2|$ is actually $3^{n-1} - 1$. If, on the other hand, the beam balances, we are left with S_3 and some standard coins (in S_1 and S_2). Thus, by Theorem 2,

$|S_3|$ can be as large as $(3^{n-1}-1)/2$. Combining these results, we find $|S|$ can be $(3^{n-1}-1)+(3^{n-1}-1)/2 = (3^n-3)/2$, as desired.

Theorem 1 shows that an underweight coin in a set of k coins can be found in $\lceil \log_3 k \rceil$ weighings where $\lceil x \rceil$ is the least integer greater than or equal to x. As can easily be seen, a standard coin (or coins) does not reduce that number. If we know only that the counterfeit coin is a different weight, then $\lceil \log_3(2k+3) \rceil$ weighings are required, as proved in Theorem 3. In that case, however, a standard coin is a help occasionally, since Theorem 2 states that $\lceil \log_3(2k+1) \rceil$ weighings are required if a standard coin is provided.

None of this actually deals with Schell's original problem, which presents us with a set of coins which *may* contain a counterfeit one or may not. We have assumed that exactly one counterfeit was present in every problem. It is easy to see, by following through the process outlined in Theorem 1, that if the beam balances on every weighing, there is exactly one coin which has never been on the scale. If we are not sure whether or not we have a counterfeit coin, that last coin is an embarrassment! Thus, exactly one fewer coins, (3^n-1), can be handled in n weighings in that case. In the procedure outlined for an "odd" coin, there is no such problem, because if all of the coins are the same weight, they will all eventually be placed on the scale.

References

Many of the early references to balancing problems were in sections devoted to problems or mathematical notes, and were untitled. We therefore list some of them in an informal way, by journal, indicating the page number and author of each article. The author is indebted to the referee for pointing out many of these references.

American Mathematical Monthly: 1945 (42, E. D. Schell; 397, M. Dernham), 1946 (156, D. Eves; 278, N. J. Fine), 1947 (46, E. D. Schell; 48, J. Rosenbaum).

Mathematical Gazette: 1945 (227, R. L. Goodstein), 1946 (231, F. S. Dyson), 1947 (31, C. A. B. Smith).

Scripta Mathematica: 1945 (360, H. D. Grossman; 361, L. Withington, Jr.), 1948 (66, C. W. Raine; 67, K. Itkin; 69, H. D. Grossman).

Geoboard Triangles with One Interior Point

CHARLES S. WEAVER
University of Illinois
Illinois State University

A geoboard is a physical model of an integer lattice, the set of points in the plane with integer coordinates. Nails are hammered in a square array on a piece of wood and rubber bands are stretched over the nails to make polygons. A central formula of geoboard geometry is Pick's formula for the area of a polygon with vertices on the lattice: Area $= T/2 + (I-1)$ where T is the number of points at which the polygon intersects the lattice and I is the number of lattice points enclosed by, but not touching, the polygon. (See [1], pp. 208–209.)

It is natural to ask what combinations of T and I can occur in polygons. For example, if $I = 0$, T can assume any value greater than 2. This can be seen by making a triangle that touches $T-1$ points on the x-axis and with third vertex on the line $y = 1$. In contrast to this is the case $I = 1$. A well-known problem states, for example, that there is no geoboard triangle touching seven lattice points and enclosing exactly one. Proofs of this fact bring together elementary geometry and number theory and reveal some of the reasons that geoboards can be fascinating. In this note we will prove a more general theorem that includes the above problem as a special case.

THEOREM. *If a geoboard triangle has T points on its boundary and exactly one point in its interior, then T equals* 3, 4, 6, 8 *or* 9.

We will prove this theorem by a sequence of lemmas beginning with some properties of integer lattices. Let L be a line in the plane passing through the origin. It consists of the set of points of the form (tx_1, tx_2) where t is arbitrary and (x_1, x_2) is a point on the line. The set is a one dimensional vector space and thus closed under addition and multiplication by constants. Since the integers are closed under addition and multiplication by integers, the set of lattice points on a line L is also closed under addition and multiplication by integers.

LEMMA 1. *Let L be a line in the plane passing through the origin. There is a lattice point (l_1, l_2) such that the set of all lattice points on L consists of the set of integral multiples, $k(l_1, l_2)$, of (l_1, l_2). Furthermore, l_1 and l_2 are relatively prime. If $(m_1, m_2) = m(l_1, l_2)$ then m is the greatest common divisor of m_1 and m_2.*

Proof. There is a unique closest distance from the origin to the other lattice points on L. To see this, look at the squares of the distances of lattice points on L to the origin. These are all integers and hence have a smallest value, d_0^2. Choose (l_1, l_2) to be one of the points at distance d_0 from the origin. Then l_1 and l_2 are relatively prime. If not, let k be a common divisor; then the point $(l_1/k, l_2/k)$ would be a point on L closer to the origin, contradicting the choice of (l_1, l_2).

Let m_1, m_2 be another lattice point on L. It is then of the form (tl_1, tl_2). Suppose t is not an integer. Let k be the largest integer smaller than t so that then the point $(m_1, m_2) - (kl_1, kl_2) = (t - k)(l_1, l_2)$ is a lattice point on L by the remarks above. Since $(t - k)$ is less than 1, the point is closer to the origin than (l_1, l_2), contrary to the way that l_1, l_2 was chosen. Hence t must be an integer. Since $m_1 = tl_1$ and $m_2 = tl_2$, t is clearly a common divisor of m_1 and m_2. If t is not the greatest common divisor consider $\gcd(m_1, m_2) = s$. Then t divides s and s/t is a common divisor of l_1 and l_2 contradicting the fact that l_1 and l_2 are relatively prime.

Now we consider a geoboard triangle. For simplicity we choose one of the vertices at the origin. The other two vertices are represented by the integer points $A = (a_1, a_2)$ and $B = (b_1, b_2)$. The two sides of the triangle coming out of the origin are represented by the vectors A and B. The third side is represented by the vector $C = (c_1, c_2) = (a_1 - b_1, a_2 - b_2)$. Let $a = \gcd(a_1, a_2)$, $b = \gcd(b_1, b_2)$, $c = \gcd(c_1, c_2)$.

LEMMA 2. *If T is the number of lattice points on the boundary of a geoboard triangle, then $T = a + b + c$.*

Proof. Let the set of lattice points on the line determined by side A be generated by the point (α_1, α_2). Applying Lemma 1, we see that the lattice points on the line are of the form $k(\alpha_1, \alpha_2)$ and the points are actually on side A when $0 \leqq k \leqq a$. Hence exactly $a + 1$ values of k give points on side A. Similar reasoning applies to each of the other two sides, so the total number of lattice points on the three sides is $a + b + c + 3$, but each of the 3 vertices is counted twice.

LEMMA 3. *If a geoboard triangle with T points on its boundary has exactly one interior point, then $a, b, c, ab, ac,$ and bc all divide T.*

Proof. Set $(a_1, a_2) = a(\alpha_1, \alpha_2)$, $(b_1, b_2) = b(\beta_1, \beta_2)$, $(c_1, c_2) = c(\gamma_1, \gamma_2)$ and compute the area of the triangle using determinants:

$$\text{area} = \frac{1}{2}\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = \frac{1}{2}\, a \cdot b \begin{vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{vmatrix} = \frac{1}{2}\, a \cdot b \cdot k, \quad \text{where} \quad k = \begin{vmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{vmatrix}.$$

By Pick's theorem, area $= T/2 + (I - 1)$. Since we assume that there is only one interior point we have $I = 1$ and the formula reduces to area $= T/2$. Equating the two expressions for the area we see that

$T = abk$; since k is an integer it follows that ab divides T. Obviously this implies that a and b divide T. The results involving c follow by choosing a different vertex of the triangle for the origin.

LEMMA 4. *If a geoboard triangle has T points on its boundary and exactly one point in its interior, then T divides* 6, 8 *or* 9.

Proof. Since, by Lemma 2, $a + b + c = T$, either a, b, or c must be greater than or equal to $T/3$. Suppose it is a. Since, by Lemma 3, a divides T, a must be either $T/2$ or $T/3$. Without loss of generality, we assume $a \geqq b \geqq c$. Then, since both b and c must also divide T, the only triples possible for (a, b, c) are: $(T/2, T/3, T/6)$, $(T/2, T/4, T/4)$ and $(T/3, T/3, T/3)$. Since ab divides T, we conclude that $T^2/6$, $T^2/8$, and $T^2/9$, respectively, must divide T. This means that T divides 6, 8 or 9.

The proof of our main theorem is now complete: only 3, 4, 6, 8 and 9 are possible values for T. All of these are in fact possible and the reader is invited to construct them.

Reference

[1] H. S. M. Coxeter, Introduction to Geometry, Wiley, New York, 1961.

Ode to the Continuum Hypothesis

MAURICE MACHOVER,
St. John's University
New York University

My name is $\aleph$ (known as c),
You have no upper bound for me [1].
I go as low as $\aleph_1$,
And then soar back restrained by none.
The hierarchies of steps I roam,
And almost every step, my home.
Of course J. König has ordained
That certain first steps can't be gained.
But Cohen and Gödel set me free,
$\aleph_\Omega$ I can be [2].
You cannot catch me in your net,
Discreteness hasn't trapped me yet.
So learn the moral of my tale,
I cannot fit into a scale.
For any scale you think will serve,
Might press me down, but then I'll swerve [3].

References

[1] K. Gödel, What is Cantor's continuum problem?, Amer. Math. Monthly, 54, 515–525. An extended version appears in P. Benacerraf and H. Putnam, Philosophy of Mathematics, Prentice-Hall, Englewood Cliffs, N. J., 1964, p. 260.

[2] A. A. Fraenkel, Y. Bar-Hillel, and A. Levy, Foundations of Set Theory, 2nd ed., North-Holland, Amsterdam, 1973, p. 104.

[3] N. Dunford and J. T. Schwartz, Linear Operators, Part III. Spectral Operators, Wiley, New York, 1971, p. 2057.

The Number of Square Matrices of a Fixed Rank

LAWRENCE VERNER
Baruch College

Let $GL(n, r; F)$ denote the set of $n \times n$ matrices of rank r with entries in a finite field F. If q is the number of elements in F, we shall determine the cardinality of the set $GL(n, r; F)$ as a function of n, r, and q using only elementary group theory and counting arguments. The result of our argument is that the cardinality of $GL(n, r; F)$ is

$$\frac{(q^n - 1)^2(q^n - q)^2 \cdots (q^n - q^{r-1})^2}{(q^r - 1)(q^r - q) \cdots (q^r - q^{r-1})}.$$

We shall partition $GL(n, r; F)$ into a collection of subsets $\mathcal{U}$, each having the same cardinality, such that the group $GL(n, F)$ of $n \times n$ matrices over F acts transitively on this partition. Thus if we fix a particular element U_0 of the partition, and let G_0 be the subgroup fixing U_0, we then have, by a standard theorem on finite transformation groups,

$$|GL(n, r; F)| = |U_0| \cdot |GL(n, F)| / |G_0|. \tag{1}$$

Now let us work out the details. Let $\mathcal{S}$ denote the set of subspaces of F^n having dimension r. If $e_1, \ldots, e_n$ is the standard basis of F^n, then the linear span S_0 of the first r vectors $e_1, \ldots, e_r$ is in $\mathcal{S}$. For each subspace S in $\mathcal{S}$ let $GL(S)$ denote the set of $n \times n$ matrices mapping F^n onto S. The collection of sets $\{GL(S): S \in \mathcal{S}\}$ is then a partition of $GL(n, r; F)$ and so $|GL(n, r; F)| = \Sigma_{S \in \mathcal{S}} |GL(S)|$.

For any $S \in \mathcal{S}$ we can pick a matrix $T \in GL(n, F)$ mapping S_0 onto S. Then the map $GL(S_0) \to GL(S)$ given by $A \to TA$ is easily seen to be a bijection. Hence we have $|GL(n, r; F)| = |GL(S_0)| \cdot |\mathcal{S}|$. $GL(S_0)$ is easily counted. It consists of all $n \times n$ matrices of rank r in which the last $n - r$ rows are all zero. Now the first row of such a matrix can have any entries except for all zeros, and so there are $q^n - 1$ possible first rows. The second row must not be a multiple of the first so there are $q^n - q$ possible second rows. The third row must not be one of the q^2 linear combinations of the first two rows so there are $q^n - q^2$ possible third rows. Continuing in this manner we obtain,

$$|GL(S_0)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{r-1}).$$

In the case $r = n$ this becomes the well-known formula

$$|GL(n, F)| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}).$$

We have already observed that left multiplication by a matrix $T \in GL(n, F)$ transforms $GL(S_0)$ into $GL(S)$, where $S = TS_0$. In other words, $GL(n, F)$ acts transitively on the partition $\{GL(S): S \in \mathcal{S}\}$: for any pair S_0, S there exists a $T \in GL(n, F)$ which takes $GL(S_0)$ to $GL(S)$. Consequently, we have $|\mathcal{S}| = |GL(n, F)| / |G_0|$ where G_0 is the subgroup of $GL(n, F)$ whose elements map S_0 to itself. To count the number of elements in G_0, consider the restriction map $G_0 \to GL(S_0)$. This map is a surjective group homomorphism whose kernel K consists of all $T \in G_0$ fixing S_0 pointwise; that is, K consists of all invertible matrices of the form

$$T = \left(\begin{array}{c|c} I_r & \\ \hline 0 & B \end{array}\right),$$

where I_r is the $r \times r$ identity matrix. Now we must have rank $T = n$. Therefore the first column of B must not be linearly dependent on the first r columns of T, which leaves $q^n - q^r$ choices; for the second column of B there are $q^n - q^{r+1}$ choices, etc. Thus we have

$$|K| = (q^n - q^r)\cdots(q^n - q^{n-1}).$$

From the first isomorphism theorem $G_0/K \cong GL(S_0) \cong GL(r, F)$, so we obtain $|G_0| = |GL(r, F)| \cdot |K| = (q^r - 1)\cdots(q^r - q^{r-1})(q^n - q^r)\cdots(q^n - q^{n-1})$. Our assertion about $|GL(n, r; F)|$ is now obtained by direct substitution of the expressions for $|GL(S_0)|$, $|GL(n, F)|$ and $|G_0|$ in (1).

Diamond Inequalities

MURRAY S. KLAMKIN
University of Alberta

ERNEST C. SCHLESINGER
Connecticut College

By a Jordan diamond $ABCD$ we shall mean a configuration of two orthogonally intersecting line segments $\overline{AC}$ and $\overline{BD}$, together with a rectifiable Jordan curve $\overset{\frown}{ABCD}$ on which the endpoints of these segments lie. Our definition does not require that the two line segments be contained in the interior of the Jordan region bounded by the curve $\overset{\frown}{ABCD}$. Thus, each of the illustrations in FIGURE 1 is an example of a Jordan diamond.

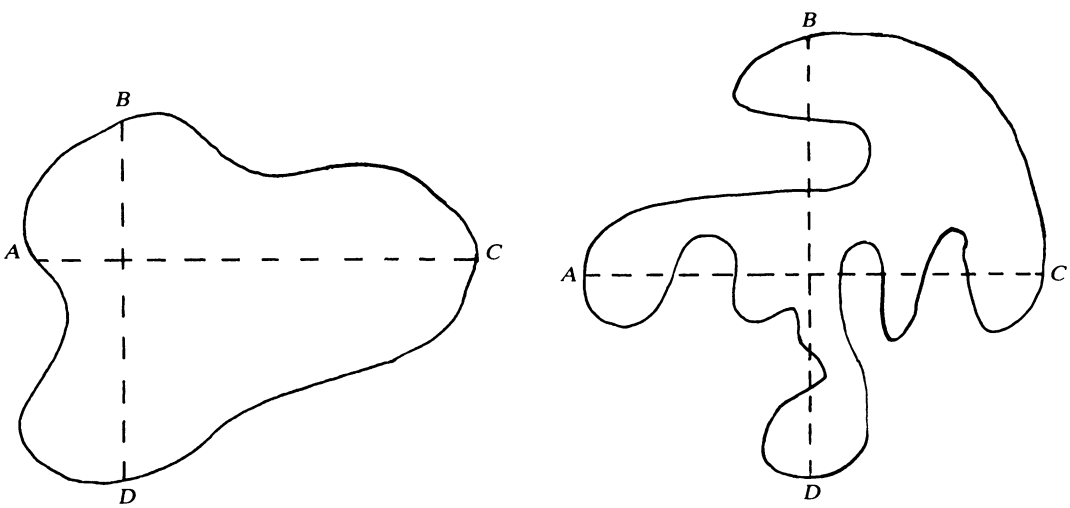


FIGURE 1.

We shall denote by PQ the length of the segment $\overline{PQ}$. Our main objective is to show that if $ABCD$ is a Jordan diamond, then

$$4(AC^2 + BD^2) \leqq L^2 \tag{1}$$

where L is the length of the Jordan curve $\overset{\frown}{ABCD}$. Since PQ is less than or equal to the length of any arc $\overset{\frown}{PQ}$, (1) will follow immediately from the quadrilateral inequality

(2) $$2\{AC^2 + BD^2\}^{1/2} \leqq AB + BC + CD + DA$$

where $\overline{AC} \perp \overline{BD}$. (Equality holds if and only if the diamond is a rhombus.)

The proof of (2) follows as an immediate consequence of the first part of the more general inequality

(3) $$2s \geqq 2(p^2 + q^2)^{1/2} \geqq (p^2 + q^2 - 2pq\cos\theta)^{1/2} + (p^2 + q^2 + 2pq\cos\theta)^{1/2} \geqq p + q \geqq s,$$

where s, p, q denote the semiperimeter and lengths of the diagonals, respectively, of a plane quadrilateral, and where θ is the angle between the diagonals. That $2s \geqq p + q \geqq s$ is well known and elementary. The middle expression $M(\theta)$ is a differentiable function on the interval $0 \leqq \theta \leqq \pi$ with its maximum value occurring at $\theta = \pi/2$ and its minimum values occurring at $\theta = 0$ and π; hence,

$$\max M(\theta) = M(\pi/2) = 2(p^2 + q^2)^{1/2}$$

$$\min M(\theta) = M(0) = |p + q| + |p - q| \geqq p + q.$$

Consequently, the proof of (3) will be completed if we show that $2s \geqq M(\theta)$ for $0 \leqq \theta \leqq \pi$.

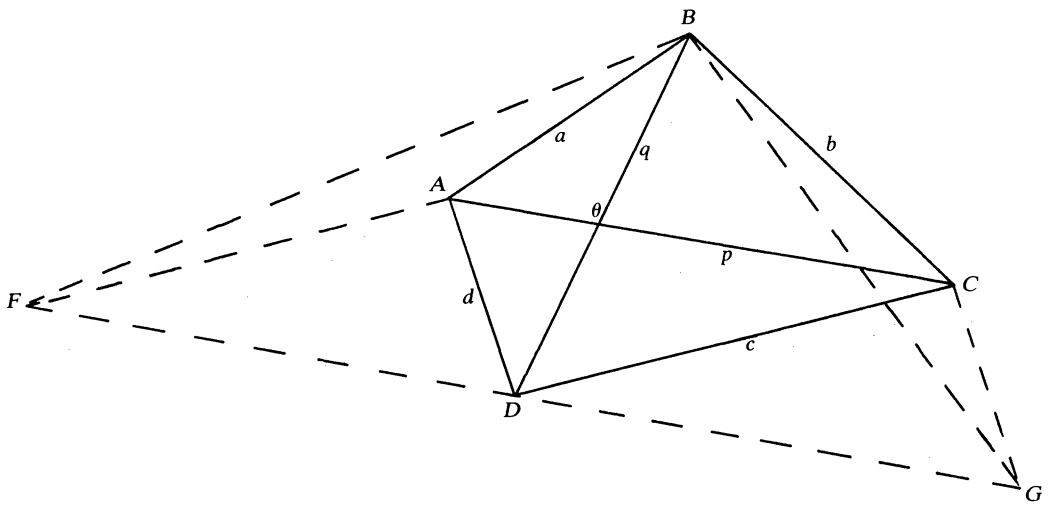


FIGURE 2.

Our proof is a geometric one for a convex quadrilateral $ABCD$ (FIGURE 2). Draw $\overline{DF}$ and $\overline{DG}$ both parallel and congruent to $\overline{AC}$. Then $ACDF$ and $ACGD$ are parallelograms, and $\sphericalangle BDF = \theta$, $\sphericalangle BDG = \pi - \theta$, $AF = c$ and $CG = d$. By the law of cosines,

$$FB^2 = p^2 + q^2 - 2pq\cos\theta, \qquad BG^2 = p^2 + q^2 + 2pq\cos\theta.$$

Finally, by the triangle inequality, $a + c \geqq FB$, and $b + d \geqq BG$, so $a + b + c + d \geqq FB + BG$. The left side of this is precisely $2s$, and the right side is $M(\theta)$, thus proving (3). Equality holds if and only if the pairs of segments $\overline{FA}, \overline{AB}$ and $\overline{BC}, \overline{CG}$ are collinear, or equivalently, if and only if $ABCD$ is a parallelogram.

In conclusion, we would like to comment briefly on the significance of the inequalities developed in this paper. Inequality (2) of this paper is a special case of a more general result of Arne Beurling. Beurling's paper [**1**] dealt with metrices of non-positive total curvature, and his proof used the subharmonic nature of the logarithm of such a metric. More recently D. Tepper, in a paper [**2**] on a conformal mapping problem, used Beurling's result in a setting that is essentially Euclidean. This gave the impetus to finding a more elementary proof.

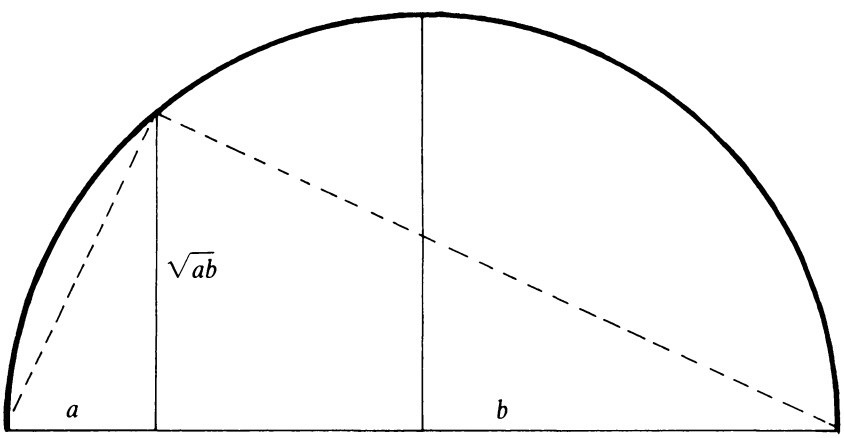
The following open question relates to our inequality (3): What are the extrema of various symmetric functions $F(p, q)$ (such as $p + q$, pq, etc.) for a quadrilateral whose sides a, b, c, and d are given in order? In this problem, the quadrilateral may or may not be restricted to being convex. If the angle θ between the diagonals is fixed, p and q may be determined as functions of a, b, c, d, and θ, but these functions are relatively complicated, and so are the restrictions on the possible values of θ for given values of the side lengths. Similar questions may also be raised concerning skew quadrilaterals.

References

[1] A. Beurling, Sur la géométrie métrique des surfaces à courbure totale $\leqq 0$. Communications du séminaire mathématique de l'Université de Lund, tome supplémentaire, dédié à Marcel Riesz, (1952) 8–11.

[2] D. E. Tepper, A theorem in conformal mapping. Arch. Rational Mech. Anal., 52 (1973) 193–198.

Proof without words: A truly geometric inequality



$$\sqrt{ab} \leqq \frac{a+b}{2}$$

— Charles Gallant
St. Francis Xavier University
Nova Scotia

PROBLEMS

DAN EUSTICE, Editor
LEROY MEYERS, Associate Editor
The Ohio State University

Proposals

To be considered for publication, solutions should be mailed before October 1, 1977.

1008. a. Let $\{a_n\}$ be an increasing sequence of positive integers and let $s_n = a_1 + a_2 + \cdots + a_n$. Show that if $\underline{\lim}\, a_n/n > 2 + \sqrt{2}$, then for all n sufficiently large there exists a perfect square between s_n and s_{n+1}.

b. Show that if the above conclusion fails and $\underline{\lim}\, a_n/n = 2 + \sqrt{2}$, then $\overline{\lim}\, a_n/n = \infty$. [*Paul Erdös, Hungarian Academy of Science, and Melvyn B. Nathanson, Southern Illinois University at Carbondale.*]

1009*. Let x, y, and n be positive integers and define $f(x) = x^2 - x + 41$ and $g(y) = y^2 - y + 68501$. Prove or disprove that n divides $g(y)$ for some y if and only if n divides $f(x)$ for some x. [*Sidney Kravitz, Dover, New Jersey.*]

1010. Prove that if the roots of a fourth degree polynomial are in arithmetic progression, then the roots of its derivative are also in arithmetic progression. [*Marius Solomon, student, University of Pennsylvania.*]

1011. Is it possible to load a pair of dice so that the probability of rolling each possible sum is 1/11? [*Richard A. Gibbs, Fort Lewis College.*]

Editor's Note: This is an old problem that we believe might be interesting to new readers.

1012. Find all solutions (x, y) of $x^y = y^{x-y}$, where x and y are positive integers. [*Gerald E. Gannon and Harris S. Shultz, California State College at Fullerton.*]

ASSISTANT EDITORS: DON BONAR, *Denison University*; WILLIAM A. MCWORTER, JR., *The Ohio State University. We invite readers to submit problems believed to be new. Proposals should be accompanied by solutions, when available, and by any information that will assist the editors. Solutions to published problems should be submitted on separate, signed sheets. An asterisk (*) will be placed by a problem to indicate that the proposer did not supply a solution. A problem submitted as a Quickie should be one that has an unexpected succinct solution. Readers desiring acknowledgement of their communications should include a self-addressed stamped card. Send all communications to this department to Dan Eustice, The Ohio State University, 231 W. 18th Ave., Columbus, Ohio 43210.*

Solutions

Absolute Primes **September 1975**

953. An absolute prime is a prime number all of whose decimal digit permutations are also prime numbers. T. N. Bhargava and P. H. Doyle, *On the existence of absolute primes*, this MAGAZINE, (47) 233–234, noted that all absolute primes of two or more digits are composed from the digits 1, 3, 7, and 9. They also proved that no absolute prime exists which uses all four of these digits. *Problem*: Show that no absolute prime number exists which contains three of the four digits 1, 3, 7, and 9. [*Allan W. Johnson, Jr., Washington, D.C.*]

Editor's Question: Are there any absolute primes of more than three digits which contain two of the digits 1, 3, 7, and 9? (See Martin Gardner, *Mathematical Games*, Scientific American, June, 1964, page 118, where the following result is discussed: decimal numbers composed entirely of 19 and 23 repetitions of the number 1 are prime.)

Solution: By way of preliminaries, we introduce the notation $PSET(I) = J$ and prove a lemma.

DEFINITIONS. Let I and J be positive non-zero integers. Define $I(k)$ to be a digit permutation of I for which $I(k) \equiv k \pmod{J}$. If there exist $I(k)$ for $k = 0, 1, 2, \ldots, J-1$, then we write $PSET(I) = J$.

Example. Bhargava and Doyle [**2**] give the example $PSET(1379) = 7$, which follows because 1379 permutes to 1379, 1793, 3719, 7913, 7193, 3197, 7139 which, on division by 7, yield remainders 0, 1, 2, 3, 4, 5, 6 respectively.

LEMMA. *Let M be an integer which can be constructed from I by adding additional digits. If $PSET(I) = J$, then the digits of M can be rearranged into a multiple of J.*

Proof. If I is L digits in length, then we can permute M into the form $N \cdot 10^L + I$ where N is some integer composed of the digits added to I. Clearly, $N \cdot 10^L \equiv n \pmod{J}$ where $0 < n \leqq J$. Because $PSET(I) = J$, we have $I(J-n) \equiv J - n \pmod{J}$. Thus, $N \cdot 10^L + I(J-n) \equiv n + J - n \equiv 0 \pmod{J}$.

There are four ways to select three different digits from 1, 3, 7, 9, viz. (1, 3, 7), (3, 7, 9), (1, 3, 9), and (1, 7, 9). We consider in turn these four cases.

Result 1. All integers composed of the digits 1, 3, 7 can be permuted to a multiple of 7.

Proof. The only three digit case is 137 which permutes to 371, a multiple of 7. Applying our lemma to the *PSET*'s in TABLE 1 completes the proof.

Result 2. All integers composed of the digits 3, 7, 9 can be permuted to a multiple of 7.

Proof. Here $973 \equiv 0 \pmod{7}$ and we have the *PSET*'s in TABLE 2.

	$I(0)$	$I(1)$	$I(2)$	$I(3)$	$I(4)$	$I(5)$	$I(6)$
$PSET(1137) = 7$:	3171	1317	1731	1137	1173	1713	1371
$PSET(3137) = 7$:	1337	1373	3173	3713	1733	7313	3317
$PSET(7137) = 7$:	3717	1737	1773	7731	7137	1377	3177

TABLE 1.

Result 3. All integers composed of the digits 1, 3, 9 can be permuted either to a multiple of 7 or to a multiple of 13.

Proof. $931 \equiv 0 \pmod 7$. The only four digit cases (1139, 3139, and 9139) permute to multiples of 13: 1391, 1339, and 3991. There are nine five-digit possibilities whose *PSET*'s are displayed in TABLE 3.

Result 4. All integers composed of the digits 1, 7, 9 can be permuted either to a multiple of 7 or to a multiple of 13.

Proof. $791 \equiv 0 \pmod 7$. The three possible four digit cases (1179, 7179, and 9179) yield these multiples of 7: 1197, 7791, and 1799. The nine *PSET*'s in TABLE 4 complete the proof.

By virtue of Results 1 through 4 we conclude

THEOREM 1. *No absolute prime exists which contains three different of the four digits* 1, 3, 7, 9.

	$I(0)$	$I(1)$	$I(2)$	$I(3)$	$I(4)$	$I(5)$	$I(6)$
$PSET(3379) = 7$:	9373	3739	3397	3937	3973	3379	3793
$PSET(7379) = 7$:	7973	3977	7793	3797	7739	7397	3779
$PSET(9379) = 7$:	3997	7939	9739	3979	9937	3799	7993

TABLE 2.

	$I(0)$	$I(1)$	$I(2)$	$I(3)$	$I(4)$	$I(5)$	$I(6)$	$I(7)$	$I(8)$	$I(9)$	$I(10)$	$I(11)$	$I(12)$
$PSET(11139) = 13$:	11193	13911	13119	11391	31191	11913	19311	39111	19131	11319	11931	11139	91311
$PSET(13139) = 13$:	19331	13391	31319	11339	31139	11393	31193	13319	13931	13139	19133	13193	11933
$PSET(19139) = 13$:	93119	19319	19931	13991	13199	11939	99131	11993	19391	13919	19913	11399	31199
$PSET(31139) = 13$:	19331	13391	31319	11339	31139	11393	31193	13319	13931	13139	19133	13193	11933
$PSET(33139) = 13$:	33319	13339	19333	13393	33193	31933	39331	33391	91333	31339	13933	31393	93313
$PSET(39139) = 13$:	31993	39391	33919	13939	19933	13993	93931	39319	19339	13399	19393	31939	93391
$PSET(91139) = 13$:	93119	19319	19931	13991	13199	11939	99131	11993	19391	13919	19913	11399	31199
$PSET(93139) = 13$:	31993	39391	33919	13939	19933	13993	93931	39319	19339	13399	19393	31939	93391
$PSET(99139) = 13$:	99931	93991	93199	19399	39199	91993	31999	93919	99913	39919	19939	13999	19993

TABLE 3.

	$I(0)$	$I(1)$	$I(2)$	$I(3)$	$I(4)$	$I(5)$	$I(6)$	$I(7)$	$I(8)$	$I(9)$	$I(10)$	$I(11)$	$I(12)$
$PSET(11179) = 13$:	11791	97111	91171	19711	11197	17191	11719	19117	71911	11917	17911	11971	11179
$PSET(17179) = 13$:	17719	11779	19177	17917	11977	17971	11797	17791	79711	19717	77191	17197	79117
$PSET(19179) = 13$:	17199	19917	91197	19971	19179	17919	11979	91917	11799	19197	71991	11997	17991
$PSET(71179) = 13$:	17719	11779	19177	17917	11977	17971	11797	17791	79711	19717	77191	17197	79117
$PSET(77179) = 13$:	17797	79717	97177	77197	19777	77719	71779	79177	17779	71977	77971	17977	77791
$PSET(79179) = 13$:	17979	79197	17799	71997	77991	17997	19779	99717	79971	19977	77919	19797	91779
$PSET(91179) = 13$:	17199	19917	91197	19971	19179	17919	11979	91917	11799	19197	71991	11997	17991
$PSET(97179) = 13$:	17979	79197	17799	71997	77991	17997	19779	99717	79971	19977	77919	19797	91779
$PSET(99179) = 13$:	19799	99971	79991	19997	91979	71999	91799	17999	79919	91997	97991	19979	99917

TABLE 4.

	$I(0)$	$I(1)$	$I(2)$	$I(3)$	$I(4)$	$I(5)$	$I(6)$
$PSET(11333) = 7$:	11333	13133	31313	13331	31133	33311	13313
$PSET(11777) = 7$:	17717	71177	71717	11777	77711	17771	17177
$PSET(11999) = 7$:	99911	11999	91919	91199	19919	19199	19991
$PSET(33111) = 7$:	31311	11313	13113	11133	13311	11331	13131
$PSET(33777) = 7$:	37737	37773	33777	73377	37377	77733	73737
$PSET(33999) = 7$:	33999	99933	39993	39399	39939	93399	93939
$PSET(77111) = 7$:	17171	17711	17117	71711	11771	11177	11717
$PSET(77333) = 7$:	37373	33377	73733	37733	33737	33773	37337
$PSET(77999) = 7$:	97979	79997	97799	99977	79979	77999	79799
$PSET(99111) = 7$:	11991	91911	19119	19911	19191	11919	11199
$PSET(99333) = 7$:	93933	33993	33399	33939	39393	39933	39339
$PSET(99777) = 7$:	79779	77799	79977	77997	79797	97977	77979

TABLE 5.

Turning to numbers composed of two different digits selected from 1, 3, 7, 9, we have

Result 5. Any integer composed of two or more of each of two digits selected from 1, 3, 7, 9 is permutable to a multiple of 7.

Proof. The only four digit possibilities are 1133, 1177, 1199, 3377, 3399, and 7799 which rearrange respectively to these multiples of 7: 3311, 1771, 9191, 3773, 9933, and 9779. The twelve *PSET*'s in TABLE 5 complete the proof.

From Result 5 we immediately obtain

THEOREM 2. *There exists no absolute prime composed of two or more of each of two digits selected from* 1, 3, 7, 9.

In view of Theorems 1 and 2 and the theorem proved in [**2**], we can state

THEOREM 3. *Let a and b represent two different digits selected from* 1, 3, 7, 9. *Then all multi-digit absolute primes take one of two forms*:

(1) $A(i) = 10^{i-1} + 10^{i-2} + \cdots + 10^1 + 10^0$,

(2) $B(i) = a \cdot A(i) + (b - a)10^j$ *where* $0 \leqq j < i$.

Beiler [**1**, Chapter XI] discusses numbers of the form $A(i)$. Using a computer, we examined numbers of the form $B(i)$, seeking to find an i beyond which $B(i)$ permutes to a composite number. We failed to find such an i but we obtained numerical results which led to

THEOREM 4. *Let* $B(i)$ *have the same meaning as in Theorem* 3 *and let* $p > 10$ *be a prime such that* $10^x \equiv 1 \pmod{p}$ *can be solved only by* $x = g(p-1)$, $g = 0, 1, 3, \ldots$. *Then for i greater than* $(p-1)$ *but not a multiple of* $(p-1)$ $B(i)$ *is permutable to a multiple of p.*

Proof. We have $B(i) = a(10^i - 1)/9 + (b - a)10^j$. Let r be the least non-negative residue of $a(10^i - 1)/9$ modulo p. Since $p > 10 > a$ and 10 is a primitive root of p, we can have $r = 0$ only if $10^i - 1 \equiv 0 \pmod{p}$, i.e., only if $(p-1) \mid i$, which is excluded by hypothesis. Hence $1 \leqq r \leqq p - 1$. Again, because 10 is a primitive root of p, the least non-negative residues $e(j)$ of the $p - 1$ numbers $(b - a)10^j$ (for $0 \leqq j \leqq p - 2$) modulo p must be distinct, and so are $1, 2, \ldots, p - 1$ in some order. Hence $e(j) = p - r$ for some j, and so $B(i)$ permutes to a multiple of p.

Theorem 4 is the basis of the following algorithm to characterize the number of digits in an absolute prime of the form $B(i)$: Let $p_1, p_2, p_3, \ldots$ be primes satisfying Theorem 4. Compute the L.C.M. of $p_1 - 1, p_2 - 1, p_3 - 1, \ldots$. Then for i greater than the largest $p - 1$, but not a multiple of their L.C.M., $B(i)$ cannot be an absolute prime.

Applying this algorithm in conjunction with a table of primitive roots [3], we use the three primes 17, 19, and 23 to show that no $B(i)$-form absolute primes exist for $16 < i < 1584$. This information with the five primes 257, 487, 491, 701, and 727 proves no $B(i)$-type absolute prime of more than 16 digits exists unless it contains a multiple of 9,220,780,800 digits. In fact, the next absolute prime of the form $B(i)$ in the list started by Bhargava and Doyle has more than nine billion digits because it turns out that no $B(i)$ $(7 \leqq i \leqq 16)$ is an absolute prime. This can be seen by considering the individual cases.

References

[1] A. H. Beiler, Recreations in the Theory of Numbers — The Queen of Mathematics Entertains, Dover, New York, 1964.

[2] T. N. Bhargava and P. H. Doyle, On the existence of absolute primes, this MAGAZINE, 47 (1974) 233.

[3] R. Osborn, Tables of All Primitive Roots of Odd Primes Less Than 1000, University of Texas Press, Austin, 1961.

ALLAN WM. JOHNSON JR.
Washington, D.C.

Partitioning the Plane **November 1975**

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

* Can the partitioning also be into three sets? [*Erwin Just, Bronx Community College.*]

Solution: Define

$$A = \left\{ \left(\frac{m}{n}, \frac{r}{s} \right) \,\middle|\, m \equiv n \equiv r \equiv s \equiv 1 \pmod 2 \right\},$$

$$B = \left\{ \left(\frac{m}{n}, \frac{r}{s} \right) \,\middle|\, m + n \equiv r \equiv s \equiv 1 \pmod 2 \right\},$$

$$C = \left\{ \left(\frac{m}{n}, \frac{r}{s} \right) \,\middle|\, m \equiv n \equiv r + s \equiv 1 \pmod 2 \right\} \quad \text{and}$$

$$D = \left\{ \left(\frac{m}{n}, \frac{r}{s} \right) \,\middle|\, m + n \equiv r + s \equiv 1 \pmod 2 \right\},$$

in which m, n, r and s are integers such that when $m \neq 0$ and $r \neq 0$, $(m, n) = (r, s) = 1$. When $m = 0$, assume $n = 1$, and when $r = 0$, assume $s = 1$. It is readily established that $A \cup B \cup C \cup D$ exhausts the set of rational points of the plane, $A \cap B = A \cap C = A \cap D = B \cap C = B \cap D = C \cap D = \varnothing$, and each of the sets A, B, C and D is dense in the plane. It will be shown that no straight line intersects all four of the sets.

Any straight line which contains two rational points may be written as $ax + by + c = 0$ in which a, b and c are integers with $(a, b, c) = 1$. If $x = m/n$ and $y = r/s$, then $ax + by + c = 0$ implies $am/n + br/s + c = 0$ or

$$(*) \qquad ams + brn + cns = 0.$$

We consider the following three cases which exhaust the possibilities for computing a, b and c (modulo 2):

(1) $a + b + c \equiv 1 \pmod 2$,

(2) $a \equiv b + c \equiv 1 \pmod 2$,

(3) $a \equiv 0 \pmod 2$, $b \equiv c \equiv 1 \pmod 2$.

It is easily found that in case (1), the equation (*) will not be satisfied by any point contained in set A; in case (2), the equation (*) will not be satisfied by any point contained in set B; and in case (3), the equation (*) will not be satisfied by any point contained in set C. It follows that the sets A, B, C and D constitute the desired partition of the rational points.

ERWIN JUST
Bronx Community College

Editors' comment. Ralph Alexander provided a reference to a paper by Paul Monsky [1] which implicitly contains a decomposition of the rational points of the plane into three dense sets so that no straight line meets all three of them. Explicitly, if the rational numbers are written in the form $2^t r/s$, where r and s are odd integers and t is an integer, then the three sets are:

$$A_1 = \left\{\left(2^u \cdot \frac{r}{s}, 2^t \cdot \frac{p}{q}\right) : u > 0 \text{ and } t > 0\right\},$$

$$A_2 = \left\{\left(2^u \cdot \frac{r}{s}, 2^t \cdot \frac{p}{q}\right) : u \leqq 0 \text{ and } u \leqq t\right\},$$

$$A_3 = \left\{\left(2^u \cdot \frac{r}{s}, 2^t \cdot \frac{p}{q}\right) : t \leqq 0 \text{ and } t < u\right\}.$$

The desired verification and a generalization to the real plane can be found in Monsky's article.

Paul Erdös comments that it is possible to decompose the plane into a continuum $\{A_\alpha\}$ of dense sets so that every line meets at most three of the A_α's. A sketch of his proof proceeds as follows: Decompose the plane into two sets A and B, both dense and both of power c in every circle and such that every line meets A in at most two points. Now let B be the first A_α and decompose A into c dense sets forming the remaining A_α. Now, clearly every line meets at most three of our sets A_α.

Reference

[1] Paul Monsky, On dividing a square into triangles, Amer. Math. Monthly, 77 (1970) 161–164.

Divisors of $n!$ **January 1976**

964. Show that every positive integer k, $k < n!$, is a sum of fewer than n distinct divisors of $n!$. [*Paul Erdös, Hungarian Academy of Science.*]

Solution: Clearly the result holds for $n = 2$. Now suppose the proposal holds for arbitrary n. Let k be a positive integer less than $(n+1)!$. By the division algorithm, $k = (n+1)q + r$, where q and r are nonnegative integers with $0 \leqq r < n+1$. Now $q < n!$ so that by the induction hypothesis, q is the sum of fewer than n distinct divisors of $n!$: $q = d_1 + d_2 + \cdots + d_p$, where $p < n$, $d_i \mid n!$, and $d_i \neq d_j$ for $i \neq j$. Thus,

$$k = (n+1)q + r = (n+1)d_1 + \cdots + (n+1)d_p + r.$$

Now, $(n+1)d_i \mid (n+1)!$ and $r \mid (n+1)!$. Hence, k is the sum of $p+1$ divisors of $(n+1)!$. If $i \neq j$, then $(n+1)d_i \neq (n+1)d_j$, so that the first p divisors are distinct. Also, $r < n+1$ implies $r < (n+1)d_i$ for $i = 1, \ldots, p$. The result is thus established by induction.

ROBERT L. HOLLIDAY
Kitzingen, Germany

Also solved by Richard Bauer, Ken Blackstein, Paul J. Campbell, Martin Cooper, Clayton W. Dodge, Marjorie Fitting, Donald C. Fuller, M. G. Greening (Australia), Richard A. Groeneveld, Earl E. Keese, Mark Kleiman, Jordan I. Levy, Gerhard Metzen (Canada), Bob Prielipp, Daniel Mark Rosenblum, Joseph H. Silverman, Edith V. Sloan, J. M. Stark, G. W. Valk, Edward T. H. Wang (Canada), Barney Weiss, Kenneth M. Wilke, and the proposer.

NEWS & LETTERS

INFINITESIMALS: SYMPOSIUM AND WORKSHOP

The University of Iowa will host a week-long workshop and symposium on Abraham Robinson's theory of infinitesimals from May 31 to June 5, 1977. Workshop sessions will deal with an introduction to the theory of infinitesimals for nonspecialists and a discussion of teaching undergraduate calculus using infinitesimals. Symposia topics will deal with applications of infinitesimal methods to probability, analysis, topology, algebra, economics and physics. The principal lecturer is H. Jerome Keisler of the University of Wisconsin, whose calculus text *Infinitesimal Calculus* is based on Robinson's theory.

Registration fee for the conference is $9.00. Dormitory accommodations are available for $8.50 (single) or $7.50 (twin) per night. Registration forms and information are available from Keith D. Stroyan, Mathematical Sciences, The University of Iowa, Iowa City, Iowa 52242; Phone: 608-263-4283.

NUMBER THEORY--PURE AND SIMPLE

The Fifth Annual Mathematics and Statistics Conference at Miami University, Oxford, Ohio will be held September 30-October 1, 1977. The theme is "Number Theory--Pure and Simple", and Professor Ivan Niven of the University of Oregon will be a featured speaker. On Friday the talks will be directed at college teachers and researchers; on Saturday they will be directed at high school teachers and students at all levels. There will be sessions for contributed papers, and abstracts should be sent to Dr. Stanley Payne, Department of Mathematics and Statistics, Miami University, Oxford, Ohio 45056. The deadline for abstracts is July 1, 1977. (Late abstracts may be considered.) Information concerning preregistration, housing, etc., may also be obtained from the above address.

CONGRESSIONAL FELLOWSHIP IN MATHEMATICAL SCIENCE

Applications are invited from candidates in the mathematical sciences for a new Congressional Science Fellowship to be supported jointly by AMS, MAA and SIAM for the twelve-month period beginning 1 September 1977. The AMS-MAA-SIAM Fellow will serve, along with three or four Fellows selected by the American Association for the Advancement of Science and half a dozen Fellows sponsored by other scientific societies, under an annual program coordinated by the AAAS. The stipend for the Fellowship is $16,000, which may be supplemented by a small amount toward relocation and travel expenses. The overall AAAS program is described in the 7 January 1977 issue of *Science*, p. 55.

Congressional Science Fellows spend their fellowship year working on the staff of an individual congressman or a congressional committee or in the congressional Office of Technology Assessment, the objective of the program being to enhance science-government interaction, the effective use of science in government, and the training of persons with scientific background for careers involving such use.

In addition to demonstrating exceptional competence in some areas of the mathematical sciences, an applicant for the AMS-MAA-SIAM Fellowship should have a broad scientific and technical background, a strong interest in the uses of the mathematical and other sciences in the solution of societal problems, and should be articulate, literate, flexible and able to work effectively with a wide variety of people.

The AMS-MAA-SIAM Congressional Science Fellowship is to be awarded competitively to a mathematically trained person at the postdoctoral to mid-career level without regard to sex, race, or ethnic group. Selection will be made by a panel of the AMS-MAA-SIAM Joint Projects Committee for Mathema-

tics, a nine-member committee consisting of three representatives from each of these organizations.

Applications should include a resume, a summary of qualifications appropriate to the position, and a statement explaining why the applicant wants to be a Congressional Science Fellow. Applicants should solicit three letters from knowledgeable persons about the applicant's competence and suitability for the award.

Applications and letters should be sent to the Conference Board of the Mathematical Sciences, 2100 Pennsylvania Ave., N.W., #832, Washington, D.C. 20037. The deadline for receipt of applications has been set at 21 May 1977.

1977 CHAUVENET PRIZE

Professor Gilbert W. Strang of the Massachusetts Institute of Technology has been awarded the 1977 Chauvenet Prize for noteworthy exposition for his paper, "Piecewise Polynomials and the Finite Element Method" (*Bull. Amer. Math. Soc.*, 79 (1973) 1128-37). This prize, represented by a certificate and an award of $500, is the twenty-fifth award of the Chauvenet Prize since its institution by the Mathematical Association of America in 1925.

Professor Strang, a 1955 graduate of M.I.T., was elected to a Rhodes Scholarship for postgraduate study in England. He was awarded First Class Honours at Balliol College, Oxford in 1957. After completing the Ph.D. degree at U.C.L.A. in 1959, under the supervision of Professor Peter Henrici, he returned to M.I.T. as a Moore Instructor and has remained at M.I.T. ever since.

His mathematical interests have centered on partial differential equations and their discrete approximations; his recent work has been concerned especially with the finite element method. His teaching has concentrated very strongly on applied linear algebra, and led in 1976 to a new undergraduate textbook, *Linear Algebra and Its Applications*.

UNDERGRADUATE RESEARCH PROGRAMS

The National Science Foundation announced recently 181 grants for Undergraduate Research Participation (URP) for the summer of 1977; seven of these programs are in mathematics. Since most of these programs accept applications from students at other institutions, we list below the project director and address for each of these seven programs. Numbers in the left margin indicate the number of available stipends: students may earn up to $900 for summer research in URP programs. Students interested in applying for these programs should communicate directly with the project directors.

4 Dr. Kim Ki-Hang Butler
Department of Mathematics
Alabama State University
Montgomery
Alabama 36101

6 Dr. Gerald L. Alexanderson
Department of Mathematics
University of Santa Clara
Santa Clara
California 95053

6 Dr. Edwin F. Stueben
Department of Mathematics
Illinois Inst. of Technology
Chicago
Illinois 60616

6 Dr. David W. Kammler
Department of Mathematics
Southern Illinois University
Carbondale
Illinois 62901

6 Dr. Joseph A. Gallian
Department of Mathematics
University of Minnesota
Duluth
Minnesota 55812

10 Dr. Robert Z. Norman
Department of Mathematics
Dartmouth College
Hanover
New Hampshire 03755

10 Dr. Hyman J. Zimmerberg
Department of Mathematics
Rutgers University
New Brunswick
New Jersey 08903

SANTOS' CONJECTURE

Concerning the recent note of Santos "Twelve and its Totitives" (this *Magazine*, November 1976, pp. 239-240), it is possible to show that for $x \geq 20.51$, there are at least 2 primes in the interval $(x, \sqrt{2x})$. This can be accomplished using the estimates of $\pi(x)$ due to Rossen and Schoenfeld (*Illinois J. Math.*, 6 (1962) 64-89), but there is probably an elementary proof along the lines of Bertrand's Postulate. The relevance of this result to Santos's article is that for $n \geq 421$, we have $\sqrt{n} \geq 20.51$, so there are always 2 primes in $(\sqrt{n}, \sqrt{2n})$ and at least one of them, say p, does not divide n. Then $(p^2, n) = 1$ and $n < p^2 < 2n$, so to verify Santos's conjecture (that 12 is the largest integer to which each of its totitives can be added to obtain a prime) we need only examine the integers up to 420. We have done this by computer search and can report that this conjecture is true.

Carl Pomerance
David E. Penney
University of Georgia
Athens
Georgia 30602

SOLUTIONS TO THE 1976 PUTNAM EXAM

In January we printed in this column questions from the 1976 Putnam Examination. To assist those who have been puzzling over these problems, we provide here hints and answers. The official report on the results of the competition, including names of winners and complete sample solutions, will be published later this year in the American Mathematical Monthly.

A-1. P is an interior point of the angle whose sides are the rays $\vec{OA}$ and $\vec{OB}$. Locate X on $\vec{OA}$ and Y on $\vec{OB}$ so that the line segment $\overline{XY}$ contains P and so that the product of distances $(PX)(PY)$ is a minimum.

Sol. Let m be the line bisecting $\angle AOB$ and let ℓ be the line perpendicular to m through P. Let X and Y be the intersections of ℓ with $\vec{OA}$ and $\vec{OB}$ respectively. Now $OX = OY$ so there is a circle C tangent to $\vec{OX}$ at X and to $\vec{OY}$ at Y. Let $\overline{X_1Y_1}$ be any other segment containing P with X_1 on $\vec{OA}$ and Y_1 on $\vec{OB}$. Let X_2 and Y_2 by the intersections of $\overline{X_1Y_1}$ with C. Then $(PX)(PY) = (PX_2)(PY_2) < (PX_1)(PY_1)$ so $(PX)(PY)$ is a minimum.

Alternatively one may construct the ray OP and let X and Y be the points of intersection of any line through P with $\vec{OA}$ and $\vec{OB}$ respectively. Differentiating and setting equal to zero a function for $(PX)(PY)$ obtained by using the law of sines on the triangles OXP and OYP shows that the minimum occurs when $OX = OY$.

A-2. Let $P(x, y) = x^2y + xy^2$ and $Q(x, y) = x^2 + xy + y^2$. For $n = 1, 2, 3, \ldots$, let $F_n(x, y) = (x + y)^n - x^n - y^n$ and $G_n(x, y) = (x + y)^n + x^n + y^n$. One observes that $G_2 = 2Q$, $F_3 = 3P$, $G_4 = 2Q^2$, $F_5 = 5PQ$, $G_6 = 2Q^3 + 3P^2$. Prove that, in fact, for each n either F_n or G_n is expressible as a polynomial in P and Q with integer coefficients.

Sol. Subtracting and adding the identities

$$(x+y)^n = (x+y)^{n-2}Q + (x+y)^{n-3}P,$$

$$x^n+y^n = (x^{n-2}+y^{n-2})Q - (x^{n-3}+y^{n-3})P$$

gives

$$F_n = QF_{n-2} + PG_{n-3}, \qquad G_n = QG_{n-2} + PF_{n-3}.$$

The result follows by induction.

A-3. Find all integral solutions of the equation

$$|p^r - q^s| = 1$$

where p and q are prime numbers and r and s are positive integers larger than unity. Prove that there are no other solutions.

Sol. Clearly either p or q is 2, so suppose $q = 2$. Then p is an odd prime with $p^r \pm 1 = 2^s$. If r is odd, $(p^r \pm 1)/(p \pm 1)$ is an odd integer which is greater than 1 since $r > 1$; this contradicts the fact that 2^s has no such factor. If r is an even in-

teger then $p^r + 1 \equiv 2 \pmod 4$ which is impossible since $s > 1$. Also, if $r = 2t$, $p^r - 1 = 2^s$ leads to $(p^t)^2 - 1 = (2n+1)^2 - 1 = 4n(n+1) = 2^s$. Since either n or $n+1$ is odd, this is only possible for $n = 1$, which implies that $s = 3$, $p = 3$, and $r = 2$.

A-4. Let r be a root of $P(x) = x^3 + ax^2 + bx - 1 = 0$ and $r + 1$ be a root of $y^3 + cy^2 + dy + 1 = 0$, where a, b, c, and d are integers. Also let $P(x)$ be irreducible over the rational numbers. Express another root s of $P(x) = 0$ as a function of r which does not explicitly involve a, b, c, or d.

Sol. Since $P(x)$ is irreducible $M(x) = P(x-1)$ is the (unique) monic irreducible polynomial for $r + 1$ over the rationals. Therefore $M(x) = x^3 + cx^2 + dx + 1$. If the zeros of P are r, s, and t, the zeros of M are $r + 1$, $s + 1$ and $t + 1$. The coefficients -1 and 1 of x^0 in P and M, respectively, tell us that $rst = 1$ and $(r+1)(s+1)(t+1) = -1$. Then $st = 1/r$, so

$$s + t = (s+1)(t+1) - st - 1$$

$$= -\frac{1}{r+1} - \frac{1}{r} - 1$$

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

Hence s is either root of

$$x^2 + \frac{r^2+3r+1}{r(r+1)}\,x + \frac{1}{r} = 0 ,$$

since $s^2 - (s+t)s + st = 0$, and these roots are $-1/(r+1)$ or $-(r+1)/r$.

A-5. In the (x, y)-plane, if R is the set of points inside and on a convex polygon, let $D(x, y)$ be the distance from (x, y) to the nearest point of R.

(a) Show that there exist constants a, b, and c, independent of R, such that

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-D(x,\,y)}\,dx\,dy = a + bL + cA,$$

where L is the perimeter of R and A is the area of R.

(b) Find the values of a, b, and c.

Sol. Let $U(t)$ consist of all the points (x, y) with $D(x, y) \le t$. Write $e^{-D(x,y)}$ as

$$\int_{D(x,y)}^{\infty} e^{-t}dt ;$$

then interchange the order of integration to transform the given integral to

$$(*) \qquad \int_{-\infty}^{\infty}\Big[\iint_{U(t)} dx\,dy\Big]e^{-t}dt .$$

The expression in brackets is just the area of $U(t)$; it can be thought of as the sum of A, the area of the region R; tL, the area of strips of length t straight out from the sides of R; and πt^2 the area of the remaining wedge shaped segments spreading out from the vertices of R. So the integral (*) is

$$\int_0^{\infty}[A+tL+\pi t^2]e^{-t}dt = A + L + 2\pi .$$

A-6. Suppose $f(x)$ is a twice continuously differentiable real valued function defined for all real numbers x and satisfying $|f(x)| \le 1$ for all x and $(f(0))^2 + (f'(0))^2 = 4$. Prove that there exists a real number x_0 such that $f(x_0) + f''(x_0) = 0$.

Sol. Let $G(x) = [f(x)]^2 + [f'(x)]^2$. Since $|f(x)| \le 1$, the Mean Value Theorem implies the existence of a and b with $-2 < a < 0 < b < 2$ such that $|f'(a)| \le 1$ and $|f'(b)| \le 1$. It follows that $G(a) \le 2$ and $G(b) \le 2$. Since $G(0) = 4$, $G(x)$ attains its maximum on $a \le x \le b$ at an interior point x_0 and hence $G'(x_0) = 2f'(x_0)[f(x_0) + f''(x_0)] = 0$. But $f'(x_0) \ne 0$ since otherwise $[f(x_0)]^2 = G(x_0) \ge 4$ and $|f(x_0)| > 1$. Thus $f(x_0) + f''(x_0) = 0$.

B-1. Evaluate

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \left([\frac{2n}{k}] - 2[\frac{n}{k}]\right)$$

and express your answer in the form $\log a - b$, with a and b positive integers. (Here $[x]$ is defined to be the integer such that $[x] \le x < [x] + 1$ and $\log x$ is the logarithm of x to base e.)

Sol. Let $f(x) = [\frac{2}{x}] - 2[\frac{1}{x}]$. Then the desired limit L equals $\int_0 f(x)dx$ where $f(x) = 0$ on $2/(2n+1) < x \leq 1/n$ and $f(x) = 1$ on $1/(n+1) < x \leq 2/(2n+1)$, for $n = 1, 2, \ldots$. Hence

$$L = (\frac{2}{3} - \frac{2}{4}) + (\frac{2}{5} - \frac{2}{6}) + \ldots$$

$$= -1 + 2(1 - \frac{1}{2} + \frac{1}{3} - \ldots)$$

$$= -1 + 2\ln 2 = \ln 4 - 1 .$$

B-2. Suppose that G is a group generated by elements A and B where $A^4 = B^7 = ABA^{-1}B = 1$, $A^2 \neq 1$, and $B \neq 1$.

(a) How many elements of G are of the form C^2 with C in G?

(b) Write each such square as a word in A and B.

Sol. Clearly $1, B, B^2, B^3, B^4, B^5, B^6$, and A^2 are distinct squares. The equations imply that every element in G can be written in the form B^iA^j, $i = 0,1,\ldots,7$, $j = 0,\ldots,3$. It is easy to show that for $i = 0,\ldots,7$, $AB^i = B^{-i}A$, and this can be used to show that $(B^iA)^2 = A^2$, $(B^iA^2)^2 = B^{2i}$, and $(B^iA^3)^2 = A^2$. Therefore the eight elements listed above are all the squares in G.

B-3. Suppose that we have n events $A_1, \ldots, A_n$, each of which has probability at least $1 - a$ of occurring, where $a < 1/4$. Further suppose that A_i and A_j are mutually independent if $|i - j| > 1$, although A_i and A_{i+1} may be dependent. Assume as known that the recurrence $u_{k+1} = u_k - au_{k-1}$, $u_0 = 1$, $u_1 = 1 - a$, defines positive real numbers u_k for $k = 0, 1, \ldots$. Show that the probability of all of $A_1, \ldots, A_n$ occurring is at least u_n.

Sol. The statement is false for $n \geq 5$ unless the hypothesis is strengthened to state that A_i is independent of the conjunction of $A_1, A_2, \ldots, A_{i-2}$ for $3 \leq i \leq n$.

B-4. For a point P on an ellipse, let d be the distance from the center of the ellipse to the line tangent to the ellipse at P. Prove that $(PF_1)(PF_2)d^2$ is constant as P varies on the ellipse, where PF_1 and PF_2 are the distances from P to the foci F_1 and F_2 of the ellipse.

Sol. Consider the point $P(x_0, y_0)$ on the ellipse $b^2x^2 + a^2y^2 = a^2b^2$, $a > b > 0$. Then $PF_1 + PF_2 = 2a$. By squaring both sides we find that $(PF_1)(PF_2) = 4a^2 - (PF_1)^2 - (PF_2)^2 = 4a^2 - [(x_0+c)^2 + y_0^2] - [(x_0-c)^2 + y_0^2] = a^2 + b^2 - x_0^2 - y_0^2$ where $c^2 = a^2 - b^2$. The equation of the tangent to the ellipse at P is $(\frac{x_0}{a^2})x + (\frac{y_0}{b^2})y - 1 = 0$, so that

$$d^2 = \left[(\frac{x_0}{a^2})^2 + (\frac{y_0}{b^2})^2\right]^{-1}$$

$$= a^4b^4/(x_0^2b^4 + y_0^2a^4)$$

$$= a^2b^2/(a^2 + b^2 - x_0^2 - y_0^2).$$

It follows that $(PF_1)(PF_2)d^2 = a^2b^2$, a constant.

B-5. Evaluate $\sum_{k=0}^{n} (-1)^k \binom{n}{k} (x - k)^n$.

Sol. The sum is $n!$ since it is the n-th difference of a monic polynomial, x^n, of degree n.

B-6. As usual, let $\sigma(N)$ denote the sum of all the (positive integral) divisors of N. Motivated by the notion of a "perfect" number, a positive integer N is called "quasiperfect" if $\sigma(N) = 2N + 1$. Prove that every quasiperfect number is the square of an odd integer.

Sol. Let $N = \Pi(p_i)^{e_i}$, a product of powers of distinct primes. Then

$$\sigma(N) = \Pi\sigma[(p_i)^{e_i}]$$

$$= \Pi[1 + p_i + p_i^2 + \ldots + (p_i)^{e_i}].$$

For $\sigma(N) = 2N + 1$, each factor of $\sigma(N)$ must be odd. Hence each odd prime p_i must have an even exponent e_i. Thus N is either a square or twice a square. If $N = 2s^2$ let 2^r be the highest power of 2 dividing N. Then $\sigma(N) = (1+2+2^2+\ldots+2^r)K = (4m+3)K$. Let p be a prime congruent to 3 mod 4 which divides $4m + 3$. Then $\sigma(N) = 2N + 1 = (2s)^2 + 1 \equiv 0 \pmod{p}$ but it is well known that -1 is not a square mod p. If N is the square of an even number, then a similar argument leads to the contradiction that -2 is a square mod p for a prime p not congruent to 1 or 3 mod 8.

Saunders Algebra Texts Point Your Students In The Right Direction!

A relevant introduction to elementary algebra

Bello & Britton: BEGINNING ALGEBRA

Real-life examples, and motivational illustrations introduce the principles of algebra. Concepts are developed step-by-step and given practical applications. Objectives statements, progress tests (with answers), and numerous problems and exercises increase comprehension. Half of the exercise answers appear at the back of the book—the other half in the accompanying **Instructor's Manual** (free upon adoption) along with four additional test sequences. A 226 page **Student Study Guide** by Donald Clayton Rose (Soft cover. $4.95. Oct. 1976.) offers additional exercises, problems and tests keyed to the text.

By **Ignacio Bello,** Hillsborough Community College; and **Jack R. Britton,** Univ. of South Florida. 435 pp. Illustd. $11.95. March 1976.

A worktext approach to elementary algebra

Groza: ELEMENTARY ALGEBRA: A Worktext

Using illustrative examples, sample problems and drills, this book provides a stimulating introduction to elementary algebra that's suitable for a variety of instructional situations. For greater teaching flexibility, chapters are broken down into sub-units which concentrate on key concepts. A separate **Teacher's Manual** containing additional test sequences and answers is also available.

By **Vivian Shaw Groza,** Sacramento City College. 728 pp. Illustd. Soft cover. $11.95. March 1975.

A motivational presentation of intermediate topics

Bello: ALGEBRA FOR COLLEGE STUDENTS

Attract and hold your students' interest with this clear, logical presentation of intermediate level topics. Its helpful marginal notes, definitions and rules are integrated throughout the text. Chapter introductions, progress tests with answers, historical notes, numerous illustrations, and worked examples reinforce the textual material. A **Student Study Guide** by James Gard (about $4.95) will be available and an accompanying **Instructor's Manual** will be free upon adoption.

By **Ignacio Bello,** Hillsborough Community College. About 385 pp., 125 ill. in two colors. About $12.50. Just Ready.

An in-depth approach to intermediate algebra

Setek: ALGEBRA: A Fundamental Approach

Using an intuitive approach to intermediate algebra, this lucid text features extensive explanations of key concepts and their modern applications. Worked examples, graded in level of difficulty, and a large number of homework problems are included. The **Instructor's Manual** with problem answers and additional chapter test sequences, is free upon adoption.

By **William M. Setek, Jr.,** Monroe Community College. About 705 pp., 215 ill. About $12.95. Just Ready.

For further information, write: **Textbook Marketing Division**

W. B. Saunders Company
West Washington Square, Philadelphia, Pa. 19105

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

MATHEMATICS MAGAZINE VOL. 50, NO. 2, MARCH 1977