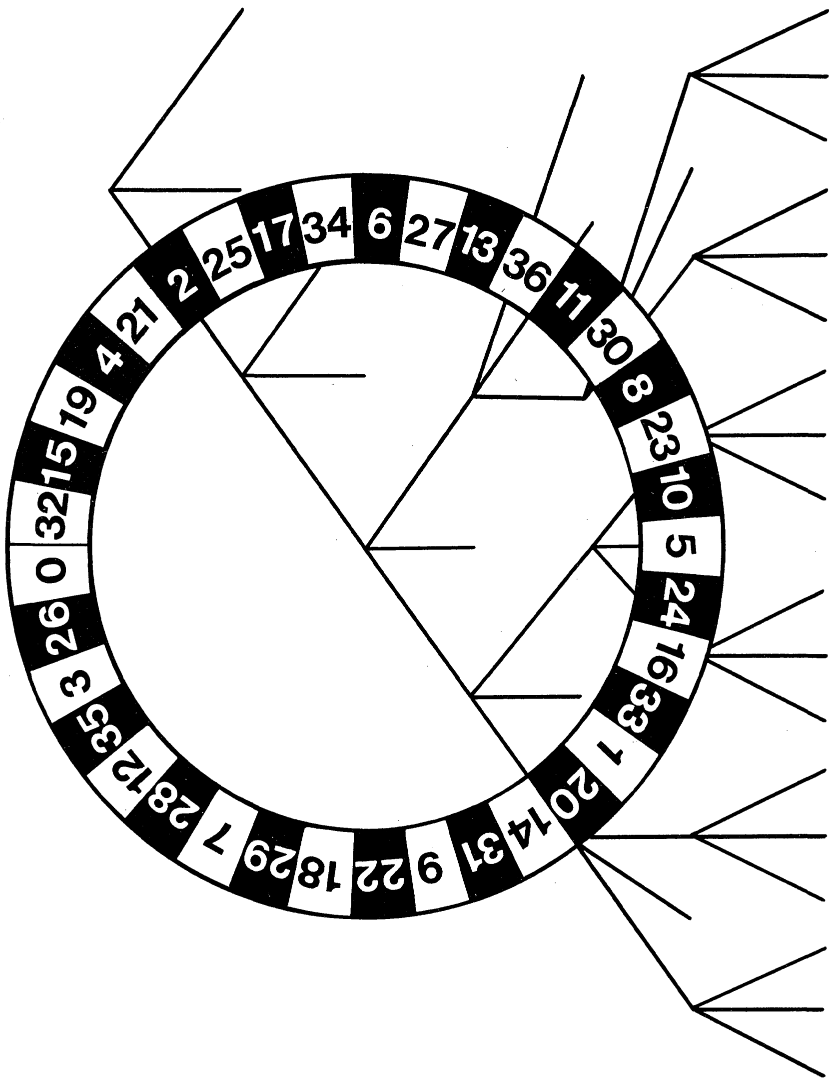
MATHEMATICS MAGAZINE



Vol. 54, No. 1
January, 1981

MARKOV CHAINS IN MONTE CARLO • G-SERIES
GROUP COUNTEREXAMPLES • HAMILTONIAN TOURS

MATHEMATICS MAGAZINE

Volume 54, Number 1, January 1981
(ISSN—0025-570X)

COVER: "Markov Chains in Monte Carlo".
Design by the Editor.

ARTICLES

NOTES

PROBLEMS

REVIEWS

NEWS AND LETTERS

EDITORIAL POLICY

Mathematics Magazine is a journal of collegiate mathematics which aims to provide inviting, informal mathematical exposition of interest to undergraduate students. Manuscripts accepted for publication in the *Magazine* should be written in a clear and lively expository style and stocked with appropriate examples and graphics. Our advice to authors is: say something new in an appealing way or say something old in a refreshing way. The *Magazine* is not a research journal and so the style, quality, and level of articles submitted for publication should realistically permit their use to supplement undergraduate courses. The editor invites manuscripts that provide insight into the history and application of mathematics, that point out interrelationships between several branches of mathematics and that illustrate the fun of doing mathematics.

New manuscripts should be sent to: Doris Schattschneider, Editor, Mathematics Magazine, Moravian College, Bethlehem, Pennsylvania 18018. 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.

Authors planning to submit manuscripts should read the full statement of editorial policy which appears in the News and Letters section of this issue of the *Magazine*. Additional copies of the policy are available from the Editor.

AUTHORS

Hans Sagan ("Markov Chains in Monte Carlo") is a Professor of Mathematics at North Carolina State University. He received his Ph.D. degree from the University of Vienna in 1950. He taught at the University of Technology of Vienna until 1954, came to the United States the same year and resumed teaching at Montana State University. He then moved to the University of Idaho before going on to North Carolina State. He is the author of a number of books on differential equations, calculus, and the calculus of variations. He is the co-author (with Carl D. Meyer, Jr.) of *Ten Easy Pieces* (Hayden Book Co., 1980), a book on computer programming. Since 1963 he has been a visiting lecturer of the Mathematical Association of America and has visited many colleges and universities in the United States and Canada. Dr. Sagan was an associate editor of *Mathematics Magazine* from 1963 to 1973 and served as a member and secretary to the Mathematical Association of America Committee on the Annual High School Mathematics Contest from 1965 to 1973. He became a U.S. Citizen in 1960. The problem that led to this article arose when the author investigated casino gambling for his most recent book, *Dry Run* (Hayden Book Co.) on systems, strategies, and computer simulations of casino games.

ILLUSTRATIONS

The two vignettes (pages 5 and 9) for "Markov Chains in Monte Carlo" were drawn by **Candy Baker**, of Bethlehem, Pennsylvania.

The illustration for "Minimum Counterexamples in Group Theory" was drawn by the Editor.

All other illustrations were provided by the authors.

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 $18 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, 1529 Eighteenth Street, N. W., Washington, D.C. 20036. Back issues may be purchased, when in print, from P. and H. Bliss Co., Middletown, Connecticut 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.

Markov Chains in Monte Carlo

A European roulette player forfeits half his stake on a zero, or may choose "prison" with a chance to recover it all. Is prison all it's cracked up to be?

HANS SAGAN
North Carolina State University
Raleigh, NC 27650

A European roulette wheel (see FIGURE 1) has 37 slots, numbered $0, 1, 2, \ldots, 36$. Excluding 0, these numbers are on black (*noir*) fields, alternating with red (*rouge*) fields; half of them are even (*pair*), half are odd (*impair*); half are low (*manque*: 1–18), and half are high (*passe*: 19–36). A *croupier* (house-man) spins the wheel and throws in an ivory ball. To back an even chance (*chance simple*) means to bet that the ball comes to rest, respectively, on a black field, or a red field, or an even number, or an odd number, or a low number, or a high number. If your chance comes up, you win even money. If the opposite chance comes up (e.g., red rather than black, odd rather than even, etc.), you lose your stake. And then there is the zero (*zéro*). The zero is what this article is all about. (In American roulette, there is a zero and a double-zero. You lose on both and that's that. What is to follow applies strictly to European roulette.)

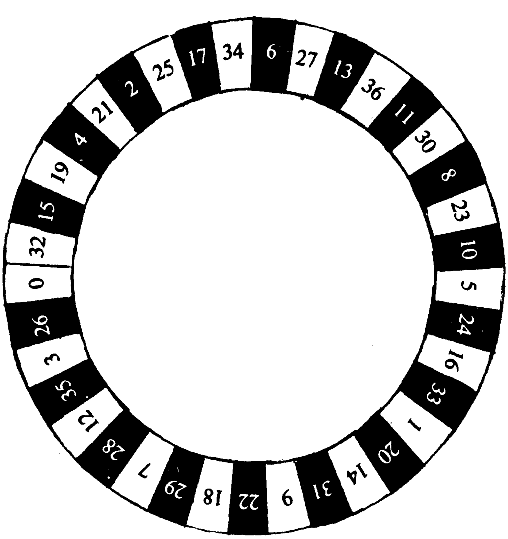


FIGURE 1

If the ivory ball comes to rest on zero, then, depending on the casino, one of the following three options may go into effect:

0. You forfeit half your stake. We call this the **0-prison option.**
1. Your stake is put in prison (*en prison*). If your chance comes up on the next turn (*coup*), you get your stake back (your stake is liberated—you break even). In all other cases (i.e., if the opposite chance comes up or the zero comes up again), then you lose your stake. We call this the **1-prison option.** The tree diagram in FIGURE 2 represents this option. S stands for "start," W for "win," L for "lose," E for "break even" and P_1 for "prison." Two "losing branches" emanate from P_1. One results from the appearance of the opposite chance, the other from the appearance of the zero.
2. Your stake is put in prison P_1 as before but, if the *coup* following imprisonment in P_1 results in a zero, your stake is put in double prison P_2. The appearance of the opposite chance or zero at the next *coup* causes the loss of your stake. If your chance comes up, however, you are moved back into P_1 and proceed as before. We call this the **2-prison option.** The tree diagram in FIGURE 3 represents this option.

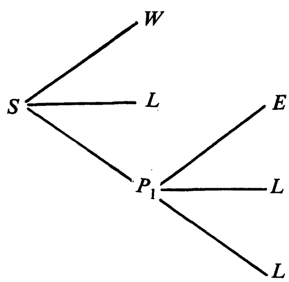


FIGURE 2

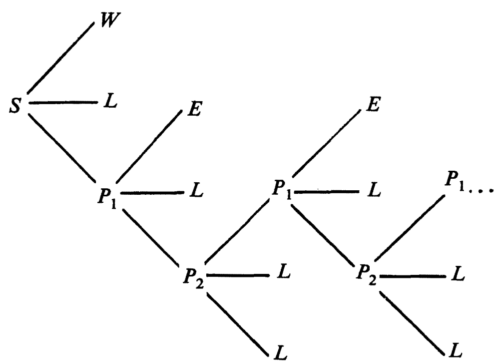
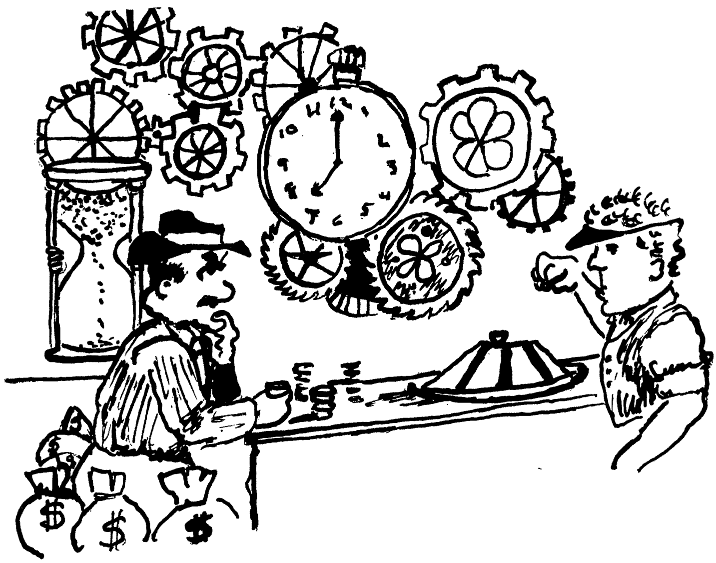


FIGURE 3

Some gaming establishments offer prisons of three degrees—presumably as a come-on for potential suckers. The (partly fallacious) reasoning probably goes as follows. Rather than lose half your stake in case of a zero, you get another chance to recover it fully in the 1-prison option, and still another chance in the 2-prison option, and still another chance in the 3-prison option, etc. Horsefeathers! Alfred Hitchcock's advice "stay out of jail" is sound. We will demonstrate in this paper that getting half your stake back on a zero is, theoretically, the best deal you can possibly get and that it does not matter much to the house how many prisons it offers. Specifically, we will show that the expected loss on 1000 successive one-dollar bets on an even chance is, with the 0-prison option, \$13.51. With the 1-prison option, however, this loss increases "sharply" to \$13.88, decreases to \$13.70 for the 2-prison option and essentially stays there, no matter how many prisons are offered. We will also show that the house-take per *coup* (one spin of the wheel with all the concomitant ballyhoo) is the same, no matter whether the house returns half the stake on a zero or offers the 1-prison option. It decreases slightly with the 2-prison option, decreases some more but almost imperceptibly with the 3-prison option and essentially stays there, no matter how many prisons are offered. On the surface, this does not seem to be quite consistent with what we said about expected losses. This is because we use different standards. What's bad for the gambler is not necessarily good for the house. The only meaningful way to compare the house-advantages for the various options is to use the house-take relative to the house's effort as a measure. Since the house's effort may be assumed to be proportional to the number of times the wheel is spun, the house-take per spin appears to be a suitable measure. On the other hand, the gambler is not interested in how many spins a specific game might last. All he is interested in is how often he has to reach into his pocket and put his dollar on the line. Hence, we decided to measure the gambler's disadvantage by using his loss per game. (This need not necessarily apply to the professional gambler who plays "around the clock." He may prefer to use the "loss per spin" as a measure and this is, of course, in magnitude equal to the "house take per spin.")



Mathematical Formulation of the Problem

Assuming that the mob has not tampered with the roulette wheel, the probability p of winning a bet on an even chance is equal to the probability of losing and both are given by $p=18/37$, while the probability z of a zero is given by $z=1/37$. The (necessarily incomplete) probability tree in FIGURE 4 represents the game with the n-prison option. Clearly, this process represents an absorbing Markov chain with the absorbing states W, L, E, P_{n+1} (P_{n+1} is also a "losing state"). We represent it by its transition matrix in canonical form,

$$\left[\begin{array}{c|c} I & 0 \\ \hline R & Q \end{array}\right] = \begin{array}{c} \begin{array}{cccc|cccccccc} W & L & E & P_{n+1} & S & P_1 & P_2 & P_3 & \cdots & P_{n-1} & P_n \end{array} \\ \left[\begin{array}{cccc|ccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ \hline p & p & 0 & 0 & 0 & z & 0 & 0 & \cdots & 0 & 0 \\ 0 & p & p & 0 & 0 & 0 & z & 0 & \cdots & 0 & 0 \\ 0 & p & 0 & 0 & 0 & p & 0 & z & \cdots & 0 & 0 \\ 0 & p & 0 & 0 & 0 & 0 & p & 0 & \cdots & 0 & 0 \\ \vdots & & & & & & & & & & \\ 0 & p & 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & z \\ 0 & p & 0 & z & 0 & 0 & 0 & 0 & \cdots & p & 0 \end{array}\right] \end{array} \begin{array}{l} W \\ L \\ E \\ P_{n+1} \\ S \\ P_1 \\ P_2 \\ P_3 \\ \vdots \\ P_{n-1} \\ P_n. \end{array}$$

The entry in the ith row and jth column represents the transition probability that the system will go from the state represented by the ith row (W, or L, or E, or P_{n+1}, or S, or $P_1,\ldots,$or P_n) to the state represented by the jth column (W, or L, or E, or P_{n+1}, or S, or $P_1,\ldots,$or P_n). For example, the entry z in the row marked P_1 and the column marked P_2 represents the probability that the stake will be put into prison P_2, coming from prison P_1.

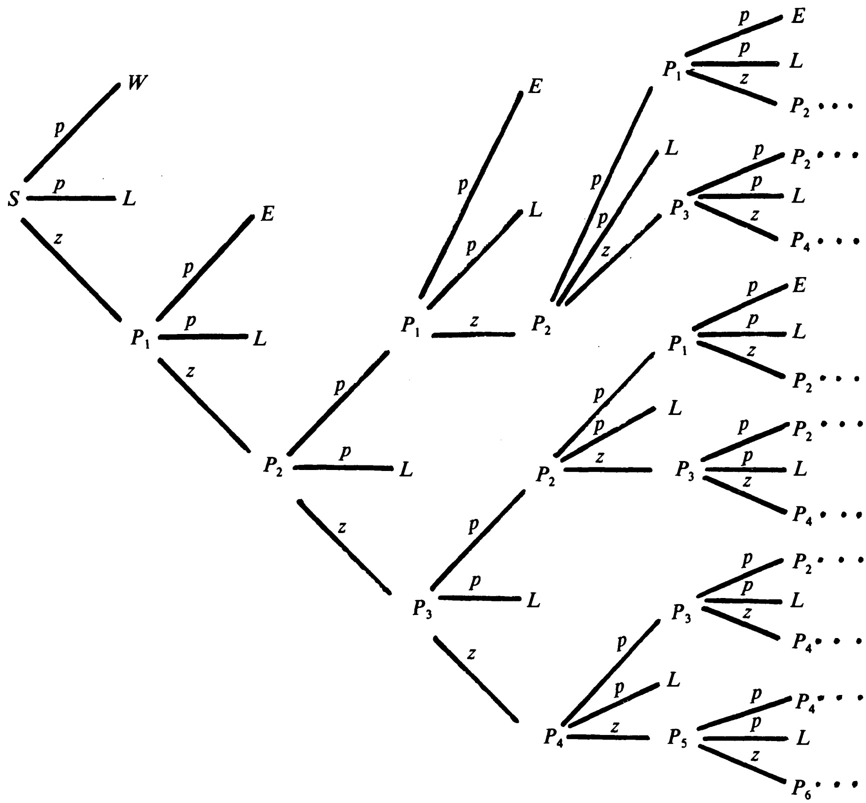


FIGURE 4

Let us establish some notation for matrices and vectors. Matrices will be denoted by capital letters, e.g., A, with i, jth entry a_{ij}. Vectors will be denoted by boldface, e.g., $\mathbf{r}$; $\mathbf{a}_0$ will denote the first row (vector) of the matrix A, since we are starting with row 0, so that $\mathbf{a}_0 = (a_{00}, a_{01}, \dots, a_{0n})$. In most cases we will be dealing with an n-prison option for fixed (but general) n. If we wish to refer explicitly to the number of prisons we will use a superscript (n), e.g., $A^{(n)}$.

The entries a_{ij} $(i, j = 0, 1, 2, \dots, n)$ of $A = (I - Q)^{-1}$ are the expected numbers of times that the system will be in the nonabsorbing state j (S, or $P_1, \dots,$ or P_n) coming from the nonabsorbing state i (S, or $P_1, \dots,$ or P_n) (see [1], p. 214ff.). Customarily, these are interpreted as average (mean) numbers of times that the system is in state j, coming from i. Hence

$$L = a_{00} + a_{01} + a_{02} + \cdots + a_{0n} \tag{1}$$

may be interpreted as the mean number of *coups* in a game with the n-prison option, that is, the mean number of times the system is in a nonabsorbing state coming from S.

If $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3, \mathbf{r}_4$ are the four columns of R, then, it may be shown (see [1], p. 217, 218) that, starting at S, $\mathbf{a}_0 \cdot \mathbf{r}_1 = a_{00} p$ is the probability of winning the game,

$$\mathbf{a}_0 \cdot (\mathbf{r}_2 + \mathbf{r}_4) = Lp + a_{0n} z \tag{2}$$

is the probability of losing the game (eventually),

$$\mathbf{a}_0 \cdot \mathbf{r}_4 = a_{0n} z \tag{3}$$

is the probability of winding up in P_{n+1}, and

$$\mathbf{a}_0 \cdot \mathbf{r}_3 = a_{01} p$$

is the probability of breaking even (eventually). Hence the expected value E of the game with the n-prison option and a one-dollar bet is

$$E=a_{00}p-Lp-a_{0n}z=-(a_{01}+a_{02}+\cdots+a_{0n})p-a_{0n}z. \tag{4}$$

Since $A(I-Q)=I$, we obtain for the elements $a_{00}, a_{01},\ldots, a_{0n}$ of the first row of A

$$\begin{aligned}
&a_{00} &&= 1\\
-&a_{00}z+a_{01}-a_{02}p &&= 0\\
&-a_{01}z+a_{02}-a_{03}p &&= 0\\
&\ddots\\
&-a_{0n-2}z+a_{0n-1}-a_{0n}p &&= 0\\
&-a_{0n-1}z+a_{0n} &&= 0.
\end{aligned} \tag{5}$$

Adding these equations for the n-prison option, recalling that $L-a_{00}=a_{01}+a_{02}+\cdots+a_{0n}$ and that $2p+z=1$, yields

$$L-a_{00}=\frac{z-a_{01}p-a_{0n}z}{p}. \tag{6}$$

From (4),

$$E=-(L-a_{00})p-a_{0n}z=-z+a_{01}p+a_{0n}z-a_{0n}z=-(z-a_{01}p). \tag{7}$$

Note that we only need the value of a_{01} to compute E for the n-prison option! (The elimination of $a_{02}, a_{03},\ldots, a_{0n-1}$ may also be accomplished by utilizing the fact that the probabilities of winning, losing, and breaking even have to add up to 1: $\mathbf{a_0}\cdot(\mathbf{r_1}+\mathbf{r_2}+\mathbf{r_3}+\mathbf{r_4})=1$, and $a_{00}=1$ follows since the probability $a_{00}p$ of winning is p.)

If N denotes the number of *coups* (spins of the wheel) in a given time period, if $H(N)$ denotes the "house-take" on these N spins (with the n-prison option), and if G denotes the number of complete games (from betting to final disposition) during these N *coups*, then the following interpretation of expected value E and mean number L of *coups* in a game is customary:

$$E\cong\frac{-H(N)}{G},\; L\cong\frac{N}{G}. \tag{8}$$

Noting that $L\geqslant 1$ and $H(N)/N\leqslant 1$, we may conclude by combining the two parts of (8) that the "house-take per *coup*" can be approximated by

$$H(N)/N\cong -E/L. \tag{9}$$

In order to support the claim which we made at the end of the introduction, we will produce values for $E^{(n)}$—as given in (7)—and for $E^{(n)}/L^{(n)}$ for several values of n, and also find their limits as n tends to infinity. From (1), $a_{00}^{(n)}=1$, (6), and (7), we have

$$-E^{(n)}/L^{(n)}=\frac{p\left(z-a_{01}^{(n)}p\right)}{p\left(1-a_{01}^{(n)}\right)+z\left(1-a_{0n}^{(n)}\right)}. \tag{10}$$

Note that we only need $a_{01}^{(n)}$ and $a_{0n}^{(n)}$ to compute this ratio!

The Solution

Let us see what happens as the number n of prisons varies. If there is no prison option ($n=0$), then the expected value of the game is $E^{(0)}=-z/2$ and the game lasts exactly one spin: $L^{(0)}=1$. Using "brute force" on the system (5) to find $a_{01}^{(n)}$ and $a_{0n}^{(n)}$ for $n=1,2,3$, we obtain

$$a_{01}^{(1)}=z,$$

$$a_{01}^{(2)}=\frac{z}{1-zp},\; a_{02}^{(2)}=\frac{z^2}{1-zp},$$

$$a_{01}^{(3)}=\frac{z-z^2p}{1-2zp},\; a_{03}^{(3)}=\frac{z^3}{1-2zp}.$$

These results led to the numerical values given in TABLE 1 for $-E^{(n)}$ and $-E^{(n)}/L^{(n)}$.

n	$-E^{(n)}$	$-E^{(n)}/L^{(n)}$
0	0.0135135135	0.0135135135
1	0.013878794	0.0135135135
2	0.013703572	0.0133286
3	0.0137012	0.0133259

TABLE 1

In the rest of this section, we will demonstrate how to find $a_{01}^{(n)}$ and $a_{0n}^{(n)}$ from equations (5) and will, without bothering to actually find these values, proceed directly to the evaluation of $\lim_{n\to\infty} a_{01}^{(n)}$ and $\lim_{n\to\infty} a_{0n}^{(n)}$. Equations (5) may be written as a linear difference equation of second order

$$-a_{0i}z+a_{0i+1}-a_{0i+2}p=0 \tag{11}$$

with the initial condition

$$a_{00}=1 \tag{12}$$

and the terminal condition

$$a_{0n}=a_{0n-1}z. \tag{13}$$

The general solution of (11) has the form $a_{0i}=Cx_1^i+Dx_2^i$, where x_1, x_2 are the two roots of the characteristic equation $px^2-x+z=0$. We find that

$$x_1=\frac{1}{2p}\left(1-\sqrt{1-4pz}\,\right),\ x_2=\frac{1}{2p}\left(1+\sqrt{1-4pz}\,\right).$$

From the initial condition (12), $a_{00}=C+D=1$, and hence, $D=1-C$. Substitution of $a_{0i}=Cx_1^i+(1-C)x_2^i$ into the terminal condition (13) yields $z(Cx_1^{n-1}+(1-C)x_2^{n-1})=Cx_1^n+(1-C)x_2^n$ and, after some cumbersome manipulations,

$$C=\frac{x_2-z}{(x_1/x_2)^n(z-x_1)+(x_2-z)}.$$

Since $|x_2|>|x_1|$, we have $\lim_{n\to\infty}(x_1/x_2)^{n-1}=0$ and hence, $\lim_{n\to\infty}C=1$. Therefore,

$$\lim_{n\to\infty} a_{01}^{(n)}=\lim_{n\to\infty}(Cx_1+(1-C)x_2)=x_1=0.02739203. \tag{14}$$

We could use the same approach to find $\lim_{n\to\infty} a_{0n}^{(n)}$ but it is easier to argue as follows. Since by (3) $a_{0n}^{(n)}z$ is the probability of winding up in P_{n+1} coming from S, since the probability of getting from S directly to P_2 is z^2, since every nonabsorbing state (beginning with the first P_2) spawns at most two nonabsorbing states (that may eventually lead to P_{n+1}), and since the probability for getting from a nonabsorbing state into another nonabsorbing state in one step is at most $(p+z)$, we have

$$a_{0n}^{(n)}z\leqslant z^2(z+p)^{n-1}=z(1/37)(19/37)^{n-1}.$$

Since $a_{0n}^{(n)}\geqslant 0$ for all n, we obtain immediately (see FIGURE 4)

$$\lim_{n\to\infty} a_{0n}^{(n)}=0. \tag{15}$$

From (14) and (15),

$$\lim_{n\to\infty}(-E^{(n)})=-(z-x_1p)=0.0137012$$

$$\lim_{n\to\infty}(-E^{(n)}/L^{(n)})=\frac{p(z-x_1p)}{p(1-x_1)+z}=0.0133259. \tag{16}$$

Interpretation of the Result

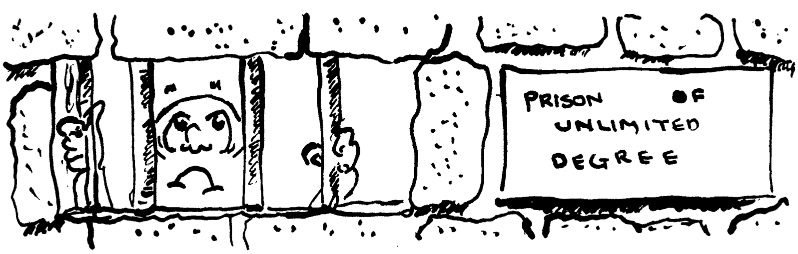
What do the numbers in TABLE 1 and in (16) mean for the gambler and what do they mean for the casino? We have taken these values and computed the expected loss of a hypothetical gambler who bets one dollar one thousand times in a row on an even chance (at a European roulette table) and the take from a hypothetical roulette wheel that is spun every 2 minutes, 8 hours a day, every day of the year (of 365 days), making 87,600 spins, assuming that somebody has always one dollar riding on an even chance. The results are compiled in TABLE 2.

n	$-E^{(n)}$	expected loss per 1000 \$1 bets	$-E^{(n)}/L^{(n)}$	house-take per 87,600 spins
0	0.0135135	\$13.51	0.0135135	\$1,183.81
1	0.013878794	\$13.88	0.0135135	\$1,183.81
2	0.013703572	\$13.70	0.0133386	\$1,167.59
3	0.0137012	\$13.70	0.0133259	\$1,167.35
⋮				
∞	0.0137012	\$13.70	0.0133259	\$1,167.35

***n*-prison option for Roulette.**

TABLE 2

If there is a moral to this story, then it seems to be this: Don't gamble—but if you can't help it and if you have a choice, ask for the return of half your stake on a *zéro*. For the casinos: Don't mess with prisons of higher than first degree, but if you do, you might buy some goodwill and just as well go all the way and offer prisons of unlimited degree.



Computer Simulation and Concluding Remarks

In order to check out the results of the preceding section, we programmed an HP 2000 to simulate a one-dollar bet on even (*pair*) at the European roulette table, permitting the operator to enter the desired number N of spins and the number of P for the P-prison option that is desired. We ran the program several times and here is what happened:

For the 1-prison option and 1,000 spins we obtained -0.054359 (vs. 0.013878794) for the loss per game and -0.053 (vs. 0.0135135) for the house take per spin. For the 2-prison option and 10,000 spins we obtained 0.0044166 (vs. 0.013703572) and 0.0043 (vs. 0.0133386) and, finally, for the 1-prison option and 87,600 spins, we obtained 0.0157145 and 0.0153082.

Good grief! These values are not anywhere near our predictions! What happened? Well, pseudo-random number generators have been known to produce lumpy pseudo-random number sequences. However, the generator that is available with the HP 2000 ACCESS BASIC has done well and produced good results in conjunction with other problems. While this does not really give us any guarantee, it does suggest that it may be worthwhile to look elsewhere for the cause of the glaring discrepancies.

It is often the case that the mean values in Markov chains are unreliable estimates. $E^{(n)}$ and $E^{(n)}/L^{(n)}$ depend on $a_{01}^{(n)}$ and $a_{0n}^{(n)}$, the mean number of *coups* that the stake is imprisoned in P_1 and in P_n, respectively. As a matter of fact, $E^{(n)}$ is a linear function of $a_{01}^{(n)}$ and $E^{(n)}/L^{(n)}$ is a rational function of $a_{01}^{(n)}$ and $a_{0n}^{(n)}$ (see (7) and (10)). Before we embark on a potentially useless investigation into the reliability of $a_{01}^{(n)}$ and $a_{0n}^{(n)}$, however, let us first check if $E^{(n)}$ and $E^{(n)}/L^{(n)}$ are sensitive to changes of $a_{01}^{(n)}$and $a_{0n}^{(n)}$ at all and if so, how sensitive they are.

To simplify the notation, let us drop the superscripts (n). Since $E(a_{01}+\Delta_1)=E(a_{01})+p\Delta_1$, where Δ_i is a small change in a_{0i},

$$(E/L)(a_{01}+\Delta_1,a_{0n}+\Delta_n)\cong(E/L)(a_{01},a_{0n})+\frac{\partial(E/L)}{\partial a_{01}}(a_{01},a_{0n})\Delta_1+\frac{\partial(E/L)}{\partial a_{0n}}(a_{01},a_{0n})\Delta_n$$

and since

$$E=-(z-a_{01}p)\cong-0.0137,\quad L=1+\frac{z}{p}-a_{01}-a_{0n}\frac{z}{p}\cong1.02,\quad p\cong0.486,$$

$$\frac{\partial E}{\partial a_{01}}=p,\quad \frac{\partial L}{\partial a_{01}}=-1,\quad \frac{\partial L}{\partial a_{0n}}=-\frac{z}{p},$$

$$\frac{\partial(E/L)}{\partial a_{01}}=\frac{pL+E}{L^2}\cong0.46,\quad \frac{\partial(E/L)}{\partial a_{0n}}=\frac{zE}{pL^2}\cong-0.00073,$$

we obtain

$$E(a_{01}+\Delta_1)=E(a_{01})+0.486\Delta_1,$$
$$(E/L)(a_{01}+\Delta_1,a_{0n}+\Delta_n)\cong(E/L)(a_{01},a_{0n})+0.46\Delta_1-0.00073\Delta_n.$$

Hence these quantities are very sensitive to changes of a_{01} but not particularly sensitive to changes of a_{0n}.

Therefore, we only need to investigate the reliability of a_{01}. For this purpose, we compute the variance $\mathrm{VAR}(t_{01})$ of the number of times t_{01} the stake is in P_1, coming from S. It will turn out that this variance is very large when compared to the square of a_{01} which means, in turn, that the mean value a_{01} is not a reliable estimate.

The variances of t_{ij} $(i,j=0,1,2,\dots,n)$, the numbers of times the system is in state j, coming from state i, are the corresponding entries of the matrix

$$A_2=A(2A_{\mathrm{diag}}-I)-A_{\mathrm{sq}}$$

(see [2], p. 49), where A_{diag} is the matrix with the diagonal elements of A and zeros elsewhere, and where A_{sq} is the matrix with the squares of the elements of A. Since we only need the second element of the first row of A_2, i.e., $\mathrm{VAR}(t_{01})$, we only need the second element a_{11} in the diagonal of A_{diag} and the second element in the first row of A_{sq}.

To find a_{11}, note that $a_{11}p$ is the probability of breaking even (eventually), starting out from P_1, while $a_{01}p$ is the probability of breaking even (eventually), starting out from S. The probability of getting from S to P_1 is z and hence, $za_{11}p=a_{01}p$ and we have $a_{11}=a_{01}/z$. Hence

$$\mathrm{VAR}(t_{01})=(a_{01})^2\left(\frac{2}{z}-1\right)-a_{01}=(a_{01})^2+\frac{a_{01}}{z}(2a_{01}-2a_{01}z-z),$$

which is very large when compared to $(a_{01})^2$, confirming our claim as to the unreliability of a_{01} and, consequently of E and E/L.

So, in the final analysis, it would appear that the sample size will have to be "very large" to come anywhere near the values in TABLE 2 and that almost anything can, and in fact does, happen to the casual gambler.

References

[1] John G. Kemeny, J. Laurie Snell, and Gerald L. Thompson, Introduction to Finite Mathematics, Prentice-Hall, Englewood Cliffs, 1974.

[2] John G. Kemeny and J. Laurie Snell, Finite Markov Chains, Van Nostrand Reinhold, New York, 1960.

Old-Fashioned Algebra Can Be Useful

HAROLD L. DORWART
Trinity College
Hartford, CT 06106

In 1919 George Pólya [6] published "Als Kuriosum" the following result. *Let $n \geqslant 17$. If among the values assumed by an integral-coefficient polynomial of degree n, the same prime integer p, with plus or minus sign, appears n times, then the polynomial is either irreducible or the product of two irreducible factors of equal degree.*

The conclusion of this theorem is intriguing, but the portion of the hypothesis that limits its applicability to polynomials of at least the 17th degree indicates why it was published as a curiosity. Fortunately new methods [**3**] have shown that this theorem is true for all odd $n>3$ and even $n>6$. These extensions were discussed and the following examples given in [**1**] to show that the theorem does not hold for $n=3$ and $n=6$:

$$(x+1)(x-1)(x+p)+p=x(x^2+px-1). \tag{1}$$

$$(x+2)(x+1)x(x-1)(x-2)(x-3)-5=(x^2-x-1)(x^4-2x^3-6x^2+7x+5). \tag{2}$$

The polynomial in (1) assumes the value p when x is ± 1 or $-p$ and it is a product of two irreducible polynomials of unequal degree. The polynomial in (2) assumes the value -5 when $x=0$, ± 1, ± 2, or 3 and it also is the product of two irreducible factors of unequal degree. We show here how these and other polynomials that do not conform to the theorem can be found.

The situation for $n=6$ is greatly simplified by the fact (see [**3**]) that for $n>5$ the polynomials of the theorem cannot assume both the values $+p$ and $-p$, and furthermore that for $n>2$ there are no polynomials of degree n that assume both $+1$ and -1 precisely $2n$ times (the maximum number possible). The only polynomial of second degree that assumes ± 1 four times is one that does so for four consecutive integral values of x. Hence without loss of generality we can write this polynomial as

$$F(x)=x(x-1)-1=(x+1)(x-2)+1=x^2-x-1, \tag{3}$$

where $F(x)$ assumes $+1$ or -1 for $x=-1,0,1,2$. Even without having seen (2), the reader would probably guess that if a sixth degree polynomial of the type considered in Pólya's theorem is to have a second degree factor, then $F(x)$ is a strong candidate by virtue of its assuming ± 1 four times.

Let us call the sixth degree polynomial $H(x)$, assume that it takes the value $-p$ six times, and assume that $F(x)$ is one factor. Then the second factor can be written as

$$G(x)=x(x-1)(ax^2+bx+c)+p. \tag{4}$$

TABLE 1 summarizes the values that each of the factors (and their product) are to assume for the following values of x: $-1,0,1,2,a_5,a_6$. If $F(a_5)=F(a_6)=p$, we must have

$$a_5(a_5-1)=1+p, \tag{5}$$

and

$$a_6(a_6-1)=1+p. \tag{6}$$

In order that $G(-1)=-p$, we must have

$$a-b+c=-p, \tag{7}$$

and from $G(2)=-p$, we obtain

$$4a+2b+c=-p. \tag{8}$$

Finally, when $G(a_5)=G(a_6)=-1$, we have

$$a_5(a_5-1)(aa_5^2+ba_5+c)=-1-p \tag{9}$$

and

$$a_6(a_6-1)(aa_6^2+ba_6+c)=-1-p. \tag{10}$$

Considering p to be an unknown along with a, b, c, a_5, a_6, we have six equations (5),...,(10) for the determination of these six unknowns. However, we are interested only in integral solutions, and the equations are of such a nature that it is by no means clear that solutions exist and, if so, that they can be found by elementary means. Fortunately some old-fashioned algebra is all that is needed.

Eliminating p between (5) and (6), we have $a_5(a_5-1)=a_6(a_6-1)$. This can be written as $a_5^2-a_6^2-(a_5-a_6)=0$ and will factor into $(a_5-a_6)(a_5+a_6-1)=0$. Thus, since $a_5\neq a_6$, we obtain

$$a_5+a_6=1. \tag{11}$$

Likewise, eliminating p between (7) and (8), we have $a-b+c=4a+2b+c$, whence

$$a=-b. \tag{12}$$

From (7), $c=b-a-p$, which when combined with (12), gives

$$c=2b-p. \tag{13}$$

We now add (5) and (9), obtaining $a_5(a_5-1)(aa_5^2+ba_5+c)+a_5(a_5-1)=0$. Substituting for c from (13), and using the fact that $a_5\neq 0,1$, we have $a_5^2+ba_5+2b-p+1=0$. If in this last expression we substitute $a=-b$ from (12) and $p=a_5(a_5-1)-1$ from (5), we obtain $-ba_5^2+ba_5+2b-a_5^2+a_5+2$. This factors to $(b+1)(a_5^2-a_5-2)$ and this in turn factors to $(b+1)(a_5-2)(a_5+1)$. Since a_5 is neither -1 or 2, we must have $b=-1$ and thus $a=1$. So far equation (10) has not been used, but if we substitute for a_6 from equation (11), we find that equation (10) reduces to equation (9) which was used.

Equations (5), (11), (13), together with $a=-b=1$, can now be used to show that

$$\begin{aligned} H(x)&=x(x+1)(x-1)(x-2)(x-a_5)(x-1+a_5)-p\\ &=(x^2-x-1)\left[x^4-2x^3-(p+1)x^2+(p+2)x+p\right]\end{aligned}$$

for primes of the form $a_5^2-(a_5+1)$, where a_5 is a positive integer >2. For $a_5=3, p=5$, yielding (1). The reader can find additional examples of sixth degree polynomials by taking $a_5=4,5,\ldots$. For $a_5=4,\ldots,9$, $a_5^2-(a_5+1)$ represents a prime.

Up to translation, the only two polynomials of first degree assuming both ± 1 are $x+1$ and $2x+1$. These can be used to investigate the polynomials of degree 3 which assume either $+p$ or $-p$ three times. To do this in an expeditious manner we take $F(x)=ax+1$, and $G(x)=x(bx+c)+p$ with values given in TABLE 2. The conditions imposed by these values are $a=\pm 1, \pm 2$, $b=-a^2$, $c=ap-2a$, $a_2=-2/a$, $a_3=(p-1)/a$, giving (1) and

$$4x(x-1)(2x+p-1)+p=(2x-1)(4x^2-4x+2px-p),$$

as well as the corresponding factorizations for polynomials assuming the value $-p$ three times.

Reducible third degree polynomials assuming a combination of $+p$ and $-p$ three times can be found by using the above procedure. Some of these, such as the polynomial $x^3-3x^2+2=(x-1)(x^2-2x-2)$, actually assume the prime four times (in this example $+2$ for $x=0,3$ and -2

for $x=-1,2$). Similar methods yield reducible fourth degree polynomials (of both types).

We conclude by mentioning several papers on closely related topics. Ore [5] has generalized the above and other results for polynomials assuming a particular prime value a certain number of times to those assuming any prime values, and has also determined the exact number of prime values a reducible polynomial can assume. Weisner [7] has obtained results for polynomials of degree n which assume the same value k (where k is any integer $\neq 0$) for n distinct values of x. And finally the writer has shown [2] that finding solutions for the equal degree decomposition in Pólya's theorem is essentially equivalent to finding *ideal* solutions in the Tarry-Escott problem [4].

	-1	0	1	2	a_5	a_6
$F(x)$	1	-1	-1	1	p	p
$G(x)$	$-p$	p	p	$-p$	-1	-1
$H(x)$	$-p$	$-p$	$-p$	$-p$	$-p$	$-p$

TABLE 1

	0	a_2	a_3
$F(x)$	1	-1	p
$G(x)$	p	$-p$	1
$H(x)$	p	p	p

TABLE 2

References

[1] H. L. Dorwart, Can this polynomial be factored?, TYCMJ, 8(1977) 67–72.

[2] ______, Concerning certain reducible polynomials, Duke Math. J., 1(1935) 70–73.

[3] H. L. Dorwart and O. Ore, Criteria for the irreducibility of polynomials, Ann. of Math., 34(1933) 81–94, 35(1934) 195.

[4] H. L. Dorwart and Warren Page, Introduction to the Tarry-Escott problem, (to appear in the forthcoming volume, TYCM Readings).

[5] O. Ore, Einige Bermerkungen Über Irreduzibilität, Jber. Deutsch. Math-Verein., 44(1934) 147–151.

[6] G. Pólya, Verschiedene Bermerkungen zur Zahlentheorie, Jber. Deutsch. Math-Verein., 28(1919) 31–40.

[7] L. Weisner, Irreducibility of polynomials of degree n which assume the same value n times, Bull. Amer. Math. Soc. (1935) 248–252.

Do Good Hands Attract?

STANLEY GUDDER
University of Denver
Denver, CO 80208

There are two different opinions about the prevalence of good hands in a poker deal. According to one player: "Every time I get a good hand, everyone else drops out and I only win a small pot." According to another: "Poker is an exciting game because there are either no good hands or many good hands in a deal."

for $x=-1,2$). Similar methods yield reducible fourth degree polynomials (of both types).

We conclude by mentioning several papers on closely related topics. Ore [5] has generalized the above and other results for polynomials assuming a particular prime value a certain number of times to those assuming any prime values, and has also determined the exact number of prime values a reducible polynomial can assume. Weisner [7] has obtained results for polynomials of degree n which assume the same value k (where k is any integer $\neq 0$) for n distinct values of x. And finally the writer has shown [2] that finding solutions for the equal degree decomposition in Pólya's theorem is essentially equivalent to finding *ideal* solutions in the Tarry-Escott problem [4].

	-1	0	1	2	a_5	a_6
$F(x)$	1	-1	-1	1	p	p
$G(x)$	$-p$	p	p	$-p$	-1	-1
$H(x)$	$-p$	$-p$	$-p$	$-p$	$-p$	$-p$

TABLE 1

	0	a_2	a_3
$F(x)$	1	-1	p
$G(x)$	p	$-p$	1
$H(x)$	p	p	p

TABLE 2

References

[1] H. L. Dorwart, Can this polynomial be factored?, TYCMJ, 8(1977) 67–72.

[2] ______, Concerning certain reducible polynomials, Duke Math. J., 1(1935) 70–73.

[3] H. L. Dorwart and O. Ore, Criteria for the irreducibility of polynomials, Ann. of Math., 34(1933) 81–94, 35(1934) 195.

[4] H. L. Dorwart and Warren Page, Introduction to the Tarry-Escott problem, (to appear in the forthcoming volume, TYCM Readings).

[5] O. Ore, Einige Bermerkungen Über Irreduzibilität, Jber. Deutsch. Math-Verein., 44(1934) 147–151.

[6] G. Pólya, Verschiedene Bermerkungen zur Zahlentheorie, Jber. Deutsch. Math-Verein., 28(1919) 31–40.

[7] L. Weisner, Irreducibility of polynomials of degree n which assume the same value n times, Bull. Amer. Math. Soc. (1935) 248–252.

Do Good Hands Attract?

STANLEY GUDDER

University of Denver

Denver, CO 80208

There are two different opinions about the prevalence of good hands in a poker deal. According to one player: "Every time I get a good hand, everyone else drops out and I only win a small pot." According to another: "Poker is an exciting game because there are either no good hands or many good hands in a deal."

Do good hands attract? That is, does the existence of one good hand increase the probability that there will be other good hands? We shall investigate this question for ordinary five-card poker. The reader is invited to use similar methods for other games of chance.

To simplify our calculations we shall restrict ourselves to some of the best hands in five-card poker. In the sequel we shall let R_i, S_i, K_i, H_i, F_i, and T_i be the events that player i is dealt a royal flush, straight flush (including royal flushes), four of a kind, full house, flush (including straight and royal), and three of a kind, respectively.

For royal flushes we have

$$P(R_i)=\frac{4}{\binom{52}{5}}=1.539\times 10^{-6}$$

$$P(R_2|R_1)=\frac{3}{\binom{47}{5}}=1.956\times 10^{-6}$$

$$P(R_3|R_1\cap R_2)=\frac{2}{\binom{42}{5}}=2.351\times 10^{-6}$$

$$P(R_4|R_1\cap R_2\cap R_3)=\frac{1}{\binom{37}{5}}=2.294\times 10^{-6}.$$

Since $P(R_2|R_1)>P(R_2)$ we say that a royal flush is **attractive**. A measure of this attraction is the **coefficient of attraction** $a(R_2,R_1)=P(R_2|R_1)/P(R_2)=1.27$. Thus, a royal flush is 1.27 times more likely given the existence of another royal flush than it otherwise would have been. The next coefficient of attraction is $a(R_3,R_1\cap R_2)=P(R_3|R_1\cap R_2)/P(R_3)=1.53$. This indicates that a royal flush is 1.53 times more likely given the existence of two other royal flushes than it otherwise would have been. The remaining coefficients of attraction are $a(R_4,R_1\cap R_2\cap R_3)=1.49$, and $a(R_i,R_1\cap\cdots\cap R_{i-1})=0$ for $i\geqslant 5$. It is interesting that although one, two, or three royal flushes are attractive, two royal flushes are more attractive than either one or three royal flushes.

We next summarize the situation for four of a kind. Since $P(K_i)=(13)(48)/\binom{52}{5}=2.401\times 10^{-4}$ and $P(K_2|K_1)=(44/48)(12)(43)/\binom{47}{5}=3.084\times 10^{-4}$, we have $a(K_2,K_1)=1.28$. Similarly, $P(K_3,K_1\cap K_2)=(44/48)(39/43)(11)(38)/\binom{42}{5}=4.085\times 10^{-4}$, so $a(K_3,K_1\cap K_2)=1.70$. Letting $a_i=a(K_{i+1},K_1\cap\cdots\cap K_i)$ we have

$$\begin{array}{lll} a_1=1.28 & a_4=3.41 & a_7=18.91 \\ a_2=1.70 & a_5=5.32 & a_8=52.46 \\ a_3=2.35 & a_6=9.23 & a_9=296.7. \end{array}$$

In this case the coefficients of attraction increase monotonically.

We list below a few other coefficients of attraction. It would be a good exercise for a class to verify these and to compute others.

$$a(F_2,F_1)=1.29\quad a(F_3,F_1\cap F_2)=1.60\quad a(F_4,F_1\cap F_2\cap F_3)=1.59$$

$$a(S_2,S_1)=1.38\quad a(H_2,H_1)=1.20.$$

Let's now consider attractions for hands of different types. For example, does a royal flush attract four of a kind? Since

$$P(K_i)=\frac{(13)(48)}{\binom{52}{5}}=2.401\times 10^{-4}$$

and

$$P(K_2|R_1)=\frac{(8)(43)}{\binom{47}{5}}=2.243\times 10^{-4},$$

we see that a royal flush *repels* four of a kind. Indeed, the coefficient of attraction is $a(K_2,R_1)=P(K_2|R_1)/P(K_2)=0.93$. However,

$$P(K_3|R_1\cap R_2)=\frac{(8)(38)}{\binom{42}{5}}=3.574\times 10^{-4},$$

so that two royal flushes attract four of a kind and $a(K_3,R_1\cap R_2)=1.49$. We find that three and four royal flushes also attract four of a kind. In fact, $a(K_4,R_1\cap R_2\cap R_3)=2.52$ and $a(K_5,R_1\cap R_2\cap R_3\cap R_4)=4.63$.

It turns out that a royal flush repels full houses, attracts flushes, and repels three of a kind: $a(H_2,R_1)=0.95$, $a(F_2,R_1)=1.30$, and $a(T_2,R_1)=0.97$.

We now answer the question that titles this paper: Do good hands attract? To be specific, let us define a **good hand** to be a full house or better. Of course, this is quite arbitrary. One could just as well define a good hand to be three of a kind or better, and the reader might try this or other definitions. However, the more types one admits as a good hand, the harder the calculations.

If G_i represents the event that player i is dealt a good hand, then $G_i=S_i\cup K_i\cup H_i$. Hence, $P(G_i)=P(S_i)+P(K_i)+P(H_i)=1.695\times 10^{-3}$. To compute $P(G_2|G_1)$ we have

$$\begin{aligned}P(G_2|G_1)&=P(S_2\cup K_2\cup H_2|S_1\cup K_1\cup H_1)\\&=P[(S_2\cup K_2\cup H_2)\cap(S_1\cup K_1\cup H_1)]/P(G_1)\\&=P(G_1)^{-1}[P(S_1)P(S_2|S_1)+P(K_1)P(K_2|K_1)+P(H_1)P(H_2|H_1)\\&\quad+2P(S_1)P(K_2|S_1)+2P(S_1)P(H_2|S_1)+2P(K_1)P(H_2|K_1)].\end{aligned}$$

After computing all the above probabilities one finds that $P(G_2|G_1)=2.063\times 10^{-3}$. Hence, one good hand attracts another, and $a(G_2,G_1)=P(G_2|G_1)/P(G_2)=1.22$. Of course, the answer could be quite different if the standard for a good hand is lowered. (One could also consider whether two good hands attract a good hand, and so forth.)

These examples motivate a theory of attraction for an arbitrary probability space. To avoid certain pathologies, we shall only consider events A such that $0<P(A)<1$. We say that an event A **attracts** an event B if $P(B|A)>P(B)$. If $P(B|A)<P(B)$ we say that A **repels** B. Since $P(B|A)=P(A\cap B)/P(A)$, we see that A attracts B if and only if $P(A\cap B)>P(A)P(B)$, and A repels B if and only if $P(A\cap B)<P(A)P(B)$. It follows that A attracts B if and only if B attracts A so attraction is a symmetric relation. Hence, we can use the terminology that A and B are **mutually attractive** instead of A attracts B. Similar terminology can be used for repulsion.

It is clear that A attracts A, so that attraction is a reflexive relation. Also, A repels A', the complement of A. More generally, if either A or B is contained in the other, then A and B are mutually attractive. Moreover, if A and B are disjoint, then A and B are mutually repulsive.

Attraction is not, however, an equivalence relation, since it is not transitive. For example, in a probability space of five points, a_1,a_2,a_3,a_4,a_5, each with equal probability, let $A=\{a_1,a_2,a_3\}$, $B=\{a_2,a_3,a_4\}$ and $C=\{a_3,a_4,a_5\}$. Then A and B are mutually attractive, as are B and C, but A and C are **not** mutually attractive. For a similar continuous example, select the unit interval $[0,1]$ as the probability space, with Lebesgue measure, and let $A=[0,\frac{1}{3}]$, $B=[\frac{1}{6},\frac{1}{2}]$, and $C=[\frac{1}{3},\frac{2}{3}]$.

We conclude with a list of good class exercises:

Problem 1. A and B are mutually attractive if and only if $P(B|A)>P(B|A')$.

Thus A and B are mutually attractive if and only if B is more likely when A has occurred than when A has not occurred.

Problem 2. A neither attracts nor repels B if and only if A and B are stochastically independent.

Problem 3. If A attracts B, then A repels B'.

Problem 4. A and B are mutually attractive if and only if A' and B' are mutually attractive.

Problem 5. If $B \cap C = \varnothing$ and A attracts both B and C, then A attracts $B \cup C$.

Problem 6. If A attracts both B and C, and A repels $B \cap C$, then A attracts $B \cup C$. Is there any example in which A attracts both B and C, but repels $B \cup C$?

Problem 7. If $B_1, \ldots, B_n$ are mutually disjoint and exhaustive ($\cup B_i = S$), and if A attracts some B_i, then A must repel some B_j.

We can define the **coefficient of attraction** for two events A and B by $a(A, B) = a(B, A) = P(A \cap B)/P(A)P(B) = P(A|B)/P(A) = P(B|A)/P(B)$. We can then use the coefficients of attraction to express Bayes' rule:

Problem 8. If $B_1, \ldots, B_n$ are mutually disjoint and exhaustive, then $\sum a(A, B_i)P(B_i) = 1$.

The author would like to thank Ron Prather for some interesting discussions on this topic.

Factorization of a Matrix Group

J. Gregory Dobbins
Mount Vernon Nazarene College
Mount Vernon, OH 43050

Matrix theory is a good source for illustrations of the basic concepts of group theory. For example, if A is any element of the group $\mathrm{GL}(n, R)$ of nonsingular $n \times n$ matrices, and $\lambda = \det A$, then whenever $\lambda^{1/n}$ is real, we can write A as $(\lambda^{-1/n}A)(\lambda^{1/n}I)$ where I is the identity matrix. Since $\det(\lambda^{-1/n}A) = 1$, the matrix $\lambda^{-1/n}A$ is in the group $\mathrm{SL}(n, R)$ of matrices with determinant 1; moreover, $\lambda^{1/n}I$ is a scalar matrix which is in the center of $\mathrm{GL}(n, R)$. Each of these subgroups is normal in G and their intersection is the subgroup $\{I, -I\}$ when n is even, and $\{I\}$ when n is odd. Thus when n is odd, it follows that $\mathrm{GL}(n, R)$ is the direct product of these two subgroups.

This factorization of A brings to mind the theorem that $\mathrm{GL}(n, K)$ is a semidirect product (where only one of the two subgroups need be normal) of the unimodular matrices $\mathrm{SL}(n, K)$ and the nonzero field elements K^* [1; 158], and motivates the following quick proof. If K is any field and $A = [a_{ij}]$ is any matrix in $\mathrm{GL}(n, K)$ with $\det(A) = \lambda$, then

$$A = \begin{bmatrix} a_{11}\cdots & a_{1n-1} & a_{1n}\lambda^{-1} \\ a_{21}\cdots & a_{2n-1} & a_{2n}\lambda^{-1} \\ \vdots & \vdots & \vdots \\ a_{n1}\cdots & a_{nn-1} & a_{nn}\lambda^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0\ldots & & 0 \\ 0 & 1\ldots & & 0 \\ \vdots & & \ddots \; 1 & \vdots \\ 0 & 0\ldots & & \lambda \end{bmatrix}.$$

The left matrix in this factorization is unimodular, whereas the right matrix is in a nonnormal subgroup H of $\mathrm{GL}(n, K)$, and H is isomorphic to K^*. Thus, the factorization of A makes the result that $\mathrm{GL}(n, K)$ is a semidirect product of $\mathrm{SL}(n, K)$ and K^* apparent. It is easy to see that the intersection of the two subgroups here is trivial.

Reference

[1] J. Rotman, The Theory of Groups: An Introduction, Allyn and Bacon, Boston, 1965.

Problem 2. A neither attracts nor repels B if and only if A and B are stochastically independent.

Problem 3. If A attracts B, then A repels B'.

Problem 4. A and B are mutually attractive if and only if A' and B' are mutually attractive.

Problem 5. If $B \cap C = \varnothing$ and A attracts both B and C, then A attracts $B \cup C$.

Problem 6. If A attracts both B and C, and A repels $B \cap C$, then A attracts $B \cup C$. Is there any example in which A attracts both B and C, but repels $B \cup C$?

Problem 7. If $B_1, \ldots, B_n$ are mutually disjoint and exhaustive ($\cup B_i = S$), and if A attracts some B_i, then A must repel some B_j.

We can define the **coefficient of attraction** for two events A and B by $a(A,B) = a(B,A) = P(A \cap B)/P(A)P(B) = P(A|B)/P(A) = P(B|A)/P(B)$. We can then use the coefficients of attraction to express Bayes' rule:

Problem 8. If $B_1, \ldots, B_n$ are mutually disjoint and exhaustive, then $\Sigma a(A, B_i)P(B_i) = 1$.

The author would like to thank Ron Prather for some interesting discussions on this topic.

Factorization of a Matrix Group

J. Gregory Dobbins
Mount Vernon Nazarene College
Mount Vernon, OH 43050

Matrix theory is a good source for illustrations of the basic concepts of group theory. For example, if A is any element of the group $\mathrm{GL}(n, R)$ of nonsingular $n \times n$ matrices, and $\lambda = \det A$, then whenever $\lambda^{1/n}$ is real, we can write A as $(\lambda^{-1/n}A)(\lambda^{1/n}I)$ where I is the identity matrix. Since $\det(\lambda^{-1/n}A) = 1$, the matrix $\lambda^{-1/n}A$ is in the group $\mathrm{SL}(n, R)$ of matrices with determinant 1; moreover, $\lambda^{1/n}I$ is a scalar matrix which is in the center of $\mathrm{GL}(n, R)$. Each of these subgroups is normal in G and their intersection is the subgroup $\{I, -I\}$ when n is even, and $\{I\}$ when n is odd. Thus when n is odd, it follows that $\mathrm{GL}(n, R)$ is the direct product of these two subgroups.

This factorization of A brings to mind the theorem that $\mathrm{GL}(n, K)$ is a semidirect product (where only one of the two subgroups need be normal) of the unimodular matrices $\mathrm{SL}(n, K)$ and the nonzero field elements K^* [1; 158], and motivates the following quick proof. If K is any field and $A = [a_{ij}]$ is any matrix in $\mathrm{GL}(n, K)$ with $\det(A) = \lambda$, then

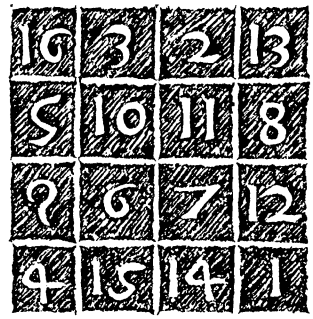
$$A = \begin{bmatrix} a_{11} \cdots & a_{1n-1} & a_{1n}\lambda^{-1} \\ a_{21} \cdots & a_{2n-1} & a_{2n}\lambda^{-1} \\ \vdots & \vdots & \vdots \\ a_{n1} \cdots & a_{nn-1} & a_{nn}\lambda^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \ldots & & 0 \\ 0 & 1 \ldots & & 0 \\ \vdots & & \ddots & \vdots \\ & & 1 & \\ 0 & 0 \ldots & & \lambda \end{bmatrix}.$$

The left matrix in this factorization is unimodular, whereas the right matrix is in a nonnormal subgroup H of $\mathrm{GL}(n, K)$, and H is isomorphic to K^*. Thus, the factorization of A makes the result that $\mathrm{GL}(n, K)$ is a semidirect product of $\mathrm{SL}(n, K)$ and K^* apparent. It is easy to see that the intersection of the two subgroups here is trivial.

Reference

[1] J. Rotman, The Theory of Groups: An Introduction, Allyn and Bacon, Boston, 1965.

Some Numerical Notes on 1981



Ask for an example of a magic square, and almost without fail, you will be shown the one at the right, which was displayed by Albrecht Dürer in his 1514 engraving "Melencolia I". With deference to Dürer, we offer a magic square for 1981. Not only does it display the date, but like Dürer's square, it possesses several extra 'magic' properties. Each of the following choices of nine numbers in the square sums to the magic constant 369: each row; each column; each diagonal of length 9, including broken (continued) diagonals; each 3×3 subsquare; the center number, 41, together with any choice of 4 pairs of numbers such that the numbers in each pair are symmetrically placed with respect to the center. The book, "New Recreations with Magic Squares", by W. H. Benson and O. Jacoby was very useful in constructing the square.

7	60	29	52	24	74	70	42	11
46	27	77	64	45	14	1	63	32
67	39	17	4	57	35	49	21	80
6	56	34	51	20	79	69	38	16
54	23	73	72	41	10	9	59	28
66	44	13	3	62	31	48	26	76
2	61	33	47	25	78	65	43	15
50	**19**	**81**	68	37	18	5	55	36
71	40	12	8	58	30	53	22	75

The magic constant 369 suggests that 1981's problems should be as simple as 1, 2, 3. After all,

$$369 = 3 \cdot 123 = 3 \cdot 100 + 2 \cdot 3 \cdot 10 + 3^2$$

$$1981 = 1 \cdot 1000 + 3^2 \cdot 100 + 2^3 \cdot 10 + 1$$

—The Editor

Simple Proofs of the Fundamental Theorem of Arithmetic

DANIEL DAVIS
University of California
Santa Cruz, CA 95060

OVED SHISHA
University of Rhode Island
Kingston, RI 02881

The purpose of this note is to give several very simple proofs of the fundamental theorem of arithmetic: *If for natural numbers a, b, c, a divides bc but is relatively prime to b, then a divides c.* The proofs are very elementary; they require only the concepts of divisibility and being relatively prime. No number theoretic result is used, not even division with a remainder!

If $S_1 = \{(a, b, c)$: a divides bc but is relatively prime to $b\}$; $S_2 = \{(a, b, c)$: a divides bc but not $c\}$; and $S_3 = S_1 \cap S_2$, then the fundamental theorem of arithmetic becomes the assertion that S_3 is the empty set. It is easy to see, for $k=1$ and 2, and hence also for $k=3$, that

A. If $(a, b, c) \in S_k$ and $b > a$, then $(a, b-a, c) \in S_k$.

B. If $(a, b, c) \in S_k$, then $\left(b, a, \frac{bc}{a}\right) \in S_k$.

In each of our proofs we derive a contradiction from the assumption that S_3 is not empty.

Proof No. 1. Let a_0 be the smallest a such that $(a, b, c) \in S_3$ for some b, c and let b_0 be the smallest b such that $(a_0, b, c) \in S_3$ for some c; say, $(a_0, b_0, c_0) \in S_3$. Since $(a_0, b_0, c_0) \in S_2$, $a_0 \neq 1$. Therefore, as $(a_0, b_0, c_0) \in S_1$, $a_0 \neq b_0$. Since, by B, $(b_0, a_0, b_0c_0/a_0) \in S_3$, we have, by the definition of a_0, $b_0 > a_0$. By A, $(a_0, b_0 - a_0, c_0) \in S_3$. But this contradicts the definition of b_0.

Proof No. 2. Let b_0 be the smallest b such that $(a, b, c) \in S_3$ for some a, c and let a_0 be the smallest a such that $(a, b_0, c) \in S_3$ for some c; say, $(a_0, b_0, c_0) \in S_3$. As in Proof No. 1, $a_0 \neq b_0$ and $(b_0, a_0, b_0c_0/a_0) \in S_3$, showing now that $a_0 > b_0$. By A, $(b_0, a_0 - b_0, b_0c_0/a_0) \in S_3$ and by B, $(a_0 - b_0, b_0, (a_0 - b_0)c_0/a_0) \in S_3$, contradicting the definition of a_0.

Proof No. 3. Let c_0 be the smallest c such that $(a, b, c) \in S_3$ for some a, b. Let b_0 be the smallest b for which $(a, b, c_0) \in S_3$ for some a; say, $(a_0, b_0, c_0) \in S_3$. As before, $a_0 \neq b_0$ and by A, $b_0 < a_0$. By B, $(b_0, a_0, b_0c_0/a_0) \in S_3$ and hence $b_0c_0/a_0 \geqslant c_0$ which is false.

Proof No. 4. Let (a_0, b_0, c_0) be an $(a, b, c) \in S_3$ for which $a+b$ is minimal. Again, $a_0 \neq b_0$. If $b_0 > a_0$, then, by A, $(a_0, b_0 - a_0, c_0) \in S_3$ which is impossible as $a_0 + (b_0 - a_0) < a_0 + b_0$. If $a_0 > b_0$, then, by B, $(b_0, a_0, b_0c_0/a_0) \in S_3$ and, by A, $(b_0, a_0 - b_0, b_0c_0/a_0) \in S_3$ which is again impossible since $b_0 + (a_0 - b_0) < a_0 + b_0$.

Proof No. 5. Let (a_0, b_0, c_0) be an $(a, b, c) \in S_3$ for which $a+b+c$ is minimal. As in the previous proof, $b_0 < a_0$. But, by B, $(b_0, a_0, b_0c_0/a_0) \in S_3$ and so, $b_0 + a_0 + (b_0c_0/a_0) \geqslant a_0 + b_0 + c_0$, implying $b_0 \geqslant a_0$.

In the relation $(a, b, c) \in S_3$, a, b and c play different roles. Proof No. 1 begins with minimizing a. To show that minimizing b or c works, we offer Proofs No. 2 and 3. In Proof No. 4 we minimize once only (namely, $a+b$) instead of twice. Finally, we include Proof No. 5 as it involves minimization of the expression $a+b+c$, symmetric in the three variables.

The theorem immediately implies that *if α, β, γ are integers and α divides $\beta\gamma$ but is relatively prime to β, then it divides γ.*

We thank Mr. Alvin Owens of Naval Research Laboratory for Proof No. 4.

Enumeration of Tours in Hamiltonian Rectangular Lattice Graphs

BASIL R. MYERS
University of Maine
Orono, ME 04469

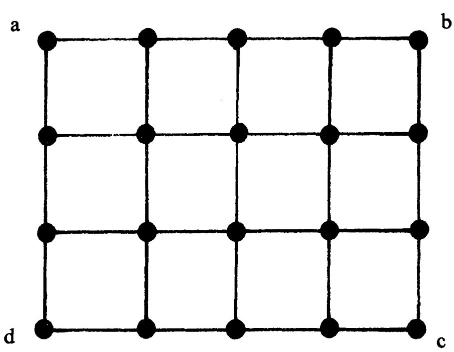
Thompson [1] uses the term **rectangular lattice graph (RLG)** for a graph whose vertices form a rectangular set of lattice points in the plane and whose arcs consist of edges between pairs of vertices that are adjacent along horizontal or vertical lines. (See FIGURE 1 for the 4×5 RLG.)

An RLG describes many physical situations: it is a graph of the network of streets in a city built on the rectangular block system; it could be the graph of an electrical communication network, the edges representing communication links between the switching centers, which are represented by the vertices. One problem of obvious interest is to know whether or not it is possible to start out at any intersection and make a tour of our rectangular city, passing through each and every intersection once en route, and returning to the starting point. When it is possible to make such a tour, the graph is said to be **hamiltonian**.

Thompson showed that a necessary and sufficient condition for an RLG to be either hamiltonian or to have a hamiltonian path is that it have an even number of vertices; and he suggested the problem of developing formulas for counting the number of tours in a hamiltonian RLG. The purpose of the present note is to describe a technique for performing that enumeration. Our technique consists of translating the problem to a simpler one where enumeration is systematic even though we do not obtain an explicit formula.

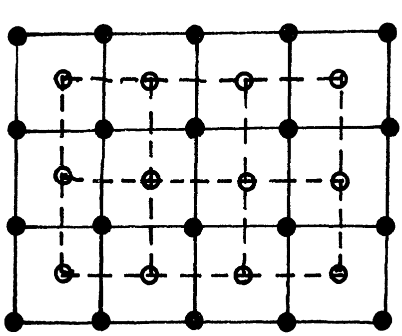
Let us begin by introducing a few basic ideas of graph theory. The **order** of a graph is the number of its vertices. The **degree** of a vertex is the number of edges incident to it. A graph is **connected** if there is a sequence of edges joining any two vertices. A connected graph in which every vertex is of degree 2 is called a **cycle**, and a connected graph without cycles is called a **tree**. For an RLG there is a cycle which contains all four **corners** (vertices of degree 2) and all the vertices of degree 3 which we call the **boundary**.

For the $h\times k$ rectangular lattice graph G there is an $(h-1)\times(k-1)$ rectangular lattice of squares (cycles of order 4), which we choose to call the **windows** of G (since they look like the windows in an $h\times k$ window frame). We may then associate with G its **window lattice graph** W whose vertices are the windows of G, two vertices being adjacent in W if and only if the two windows of G which are these vertices have a common edge. (See FIGURE 2, in which the 3×4



4×5 rectangular lattice graph.

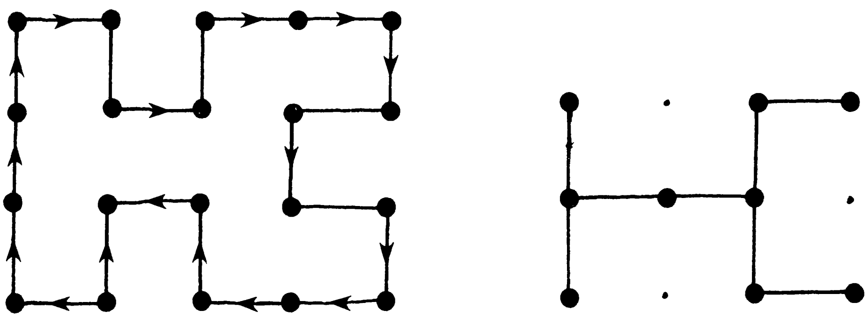
FIGURE 1



3×4 window lattice (broken lines) associated with the 4×5 lattice (solid lines).

FIGURE 2

window lattice graph is shown superimposed on the 4×5 RLG it is associated with.) Suppose that G is hamiltonian and that H is a tour of G. (From here on we assume $h > 2$ and $k > 2$ so as to exclude the trivial case of an RLG at least one of whose dimensions is 2, which has its boundary as its only tour.) We can always start on a tour at the corner vertex a, proceed to the right along the edge joining a to its horizontally adjacent vertex, and thenceforth, return eventually to a. Suppose that we orient the hk edges of the tour H by placing arrowheads on them in the direction of traversal, as we proceed. (See FIGURE 3(a) as an example of an oriented tour of a 4×5 RLG.) We define the **interior** of the oriented tour to be the region to the right of and enclosed by the edges of the tour as we traverse it. Since G is hamiltonian, there can be no vertices of G in the interior of the tour; and since the tour is a cycle, there can be no "holes" in its interior. The interior is thus a connected region and the subgraph T_H of the window lattice W of G that is associated with H is connected, but can have no cycles, and is therefore a tree. It is obvious that H does not contain the boundary of G and hence that T_H does not span W. (See FIGURE 3(b) which shows the tree T_H associated with the tour H of FIGURE 3(a).) *Each tour H of G is thus uniquely represented by the associated nonspanning tree T_H of the window lattice graph of G.*



(a) **Oriented tour of a 4×5 RLG.**

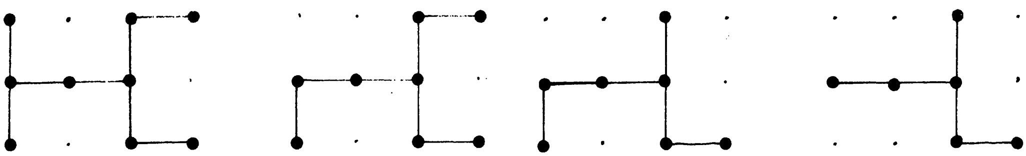
(b) **Tree of the window lattice associated with the tour on the left.**

FIGURE 3

LEMMA. *The order of T_H is $\frac{1}{2}hk - 1$.*

Proof. There are at least two vertices of degree 1 in any tree **[3]**. It follows immediately that if v_1 is a vertex of degree 1 in a tree T, then the graph $T' = T - v_1$, which results on deleting v_1 and the edge incident with it from T, is also a tree, so that T' contains a vertex v_1' of degree 1. The graph $T'' = T' - v_i'$ is similarly a tree. Thus, any tree T can be reduced to a single vertex (the trivial graph) by successive removals of a vertex of degree 1 from the tree subgraph which remains at each stage. The order of T is one plus the number of such removals.

Now consider the tree T_H of the window graph W which is associated with the tour H of the hamiltonian rectangular lattice G. The tour H spans all of the vertices of G and is thus of order hk. None of the edges in the interior of H is incident with any of the four corner vertices of G. Suppose we remove a vertex v_1 of degree 1 from the tree T_H associated with H, to form a tree $T_H' = T_H - v_1$, which has one less edge than T_H. There is a window w_1 of G associated with v_1. Let H' be the "subtour" defined by T_H'. Since T_H' is a tree, the interior of H' is a connected subregion of the interior of H, and contains one less window of G (the window w_1) than the interior of G. Further, H' is of order 2 less than H and has one less edge of G in its interior than does H. We continue this reduction process until the tree T_H is reduced to a single vertex v_p, the "subtour" which associates v_p with G being a single window v_p of G, of order 4. Since at each step there is a reduction in order of 2 in successive "subtours," and since the total reduction in order is $hk-4$, the number of steps in the reduction to v_p is $\frac{1}{2}(hk-4)$. Since there is one less interior edge in successive "subtours," this then is also the number of edges of T_H, so that T_H is of order $\frac{1}{2}(hk-4)+1=\frac{1}{2}hk-1$. (See FIGURE 4 for an illustration of the first three of one possible set of reductions of the tree T_H of FIGURE 3(b).) This proves the lemma.



Successive reductions of the tree of FIGURE 3(b).

FIGURE 4

We now present a set of conditions which characterizes the tree T_H associated with a tour H. Each tree T_H associated with a tour satisfies the following five properties.

(i) T_H contains the four corners of W.

(ii) For v_1, v_2 any pair of vertices which are adjacent in W and are in T_H, the edge joining them in W is also in T_H since the windows w_1, w_2 of G which correspond respectively to v_1, v_2 are then adjacent in G and are thus both in the interior of the tour H of G with which T_H is associated. It follows immediately that not all four of the vertices of a window of W can be in any T_H, since then T_H would contain a cycle of order 4, which is not possible since it is a tree.

(iii) T_H cannot contain a diagonally-opposite pair of vertices of a window of W unless it also contains a third vertex of that window. For suppose v_1, v_3 are such a pair of vertices. The windows w_1, w_3 of G corresponding respectively to these vertices have a vertex v_c in common in G; v_c would have degree 4 in the tour which has these two windows in its interior, which is not possible, since the degree of each vertex in a tour is 2.

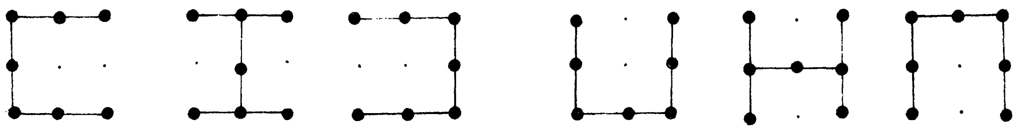
(iv) T_H must contain at least one of each pair of vertices that are adjacent on the boundary of W.

(v) T_H is of order $\frac{1}{2}hk-1$.

Conversely, each tree T_H of W which has these properties evidently defines a unique tour H in G; and, as noted previously, each tour H of G is uniquely represented by its associated tree T_H of W.

The correspondence between tours and trees allows enumeration of the set $\{H\}$ of the tours of G by enumerating the set $\{T_H\}$ of the nonspanning trees of the associated window lattice W, each T_H of which has the above properties. This enumeration is easily performed by hand for low-order rectangular lattice graphs. We illustrate for the set of $4\times k$ graphs and give the detailed computation for the 4×7 lattice. In the process we shall introduce a binary code which will help with this combinatorial problem.

For a tour H of the 4×4 lattice, the associated window lattice has dimensions 3×3 and the associated tree T_H of W spans seven of the nine vertices of W. There are six such trees, shown in FIGURE 5. The binary number shown in parentheses with each of the trees in FIGURE 5 is a classification according to the existence and position of "vertical" paths of maximum order 3 (the vertical dimension of the window lattice W). The conditions on T_H dictate that there must be at least one such vertical path in each tree T_H corresponding to a tour H in a $4\times k$ RLG,



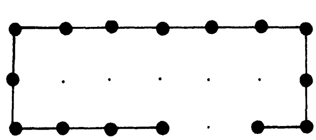
(100) (010) (001) (101) (101) (101)

The trees in the 3×3 window lattice associated with the six tours of the 4×4 RLG.

FIGURE 5

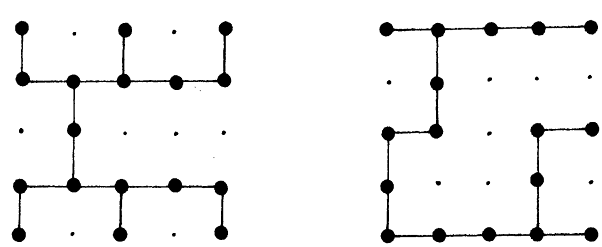
irrespective of the value of k, and hence that there is no tree with the code 000. To see this note that since T_H is a tree and is therefore connected, there must be a path joining each vertex of T_H which is in the top row of W to each vertex of T_h which is in the bottom row of W. This observation along with conditions (i) and (iv) verifies the assertion. (For $h>4$, $k>4$ there will, however, be at least one tree T_H with an all-zeros code.)

In general, every code length will be $k-1$, and there will be trees for each binary number of this length that has no pair of 1's adjacent. For example, for $k=7$ there are six codes each with a single 1 digit, four with the block 101 plus three zeros, three with the block 1001 plus two zeros, two with the block 10001, one with 100001, two with 10101, and two with 101001, and no others, to be considered. We observe that the number of trees with a given code depends only on the sub-block from the first 1 in sequence to the last 1 in the code. For example, just as there are exactly three trees with the code 101 in the 3×3 window lattice, so also are there exactly three trees with the code 001010000 in the 3×10 window lattice. To each code with a single 1, there is exactly one tree. And to a code-block of length m which has a 1 at each end, plus $m-2$ zeros, it is not difficult to see that there are $2(m-2)$ trees T_H when $m-2>1$, and three trees T_H for the code 101 ($m-2=1$). For example, one of the ten trees with the code 1000001 is shown in FIGURE 6, the other nine being evident symmetries of this one. The number of trees with a code block containing more than two 1's is evidently the product of the numbers for the sub-blocks each with two 1's. For example, the number of trees with the code 10010000101 is $4\times8\times3=96$.



1000001-code tree.

FIGURE 6



(a) (b)

00000-code trees.

FIGURE 7

We show in TABLE 1 the computation of the ninety-two trees T_H in the 3×6 window lattice, where the weights are the numbers of trees for the respective code blocks. There are thus ninety-two tours of the 4×7 rectangular lattice. The following table gives the numbers of tours of the $4\times k$ lattice, for $k=2,3,\ldots,8$.

k	2	3	4	5	6	7	8
No. of tours	1	2	6	14	37	92	236

3×6 window lattice

code block	weight	No. of codes with block	No. of trees = weight × number
1	1	6	6
101	3	4	12
1001	4	3	12
10001	6	2	12
10101	9	2	18
100001	8	1	8
101001	12	2	24
			92

TABLE 1

The combinatorial problem in the general case is that of having to determine all admissible distributions of the known number of vertices of the W-lattice vertex matrix. For example, FIGURE 7(a) shows a tree T_H with the all-zeros code 00000 in the 5×5 window lattice where the eight vertices of W not spanned by T_H are distributed in accord with the composition 12131 of 8 among the columns of W, and FIGURE 7(b) shows another code-00000 tree T_H where the 8 nonspanned vertices are distributed as the composition 11312.

References

[1] Gerald L. Thompson, Hamiltonian tours and paths in rectangular lattice graphs, this MAGAZINE, 50 (1977) 147–150.

[2] Frank Harary, Graph Theory, Addison-Wesley, Reading, MA, 1969.

[3] S. Seshu and M. B. Reed, Linear Graphs and Electrical Networks, Addison-Wesley, Reading, MA, 1961; Problem No. 2-6, p. 33.

Minimum Counterexamples in Group Theory

DESMOND MACHALE
University College
Cork, Ireland

In the theory of finite groups, many major theorems have been proved by the minimum counterexample technique which works as follows. If there is a counterexample to a given theorem, then there is a counterexample G of smallest possible order. The assumption that G exists is then used to force a contradiction and the theorem in question is thus established. In practice, the contradiction frequently arises from the existence of a counterexample of order smaller than that of the presumed minimum counterexample. This technique was used by G. A. Miller **[1]**, as early as 1916, though it may have been used by earlier writers. Of course, the minimum counterexample technique is merely a disguised form of mathematical induction and in fact bears the same kind of relation to induction as does proof by the method of infinite descent used in number theory.

3×6 window lattice

code block	weight	No. of codes with block	No. of trees = weight × number
1	1	6	6
101	3	4	12
1001	4	3	12
10001	6	2	12
10101	9	2	18
100001	8	1	8
101001	12	2	24
			92

TABLE 1

The combinatorial problem in the general case is that of having to determine all admissible distributions of the known number of vertices of the W-lattice vertex matrix. For example, FIGURE 7(a) shows a tree T_H with the all-zeros code 00000 in the 5×5 window lattice where the eight vertices of W not spanned by T_H are distributed in accord with the composition 12131 of 8 among the columns of W, and FIGURE 7(b) shows another code-00000 tree T_H where the 8 nonspanned vertices are distributed as the composition 11312.

References

[1] Gerald L. Thompson, Hamiltonian tours and paths in rectangular lattice graphs, this MAGAZINE, 50 (1977) 147–150.

[2] Frank Harary, Graph Theory, Addison-Wesley, Reading, MA, 1969.

[3] S. Seshu and M. B. Reed, Linear Graphs and Electrical Networks, Addison-Wesley, Reading, MA, 1961; Problem No. 2-6, p. 33.

Minimum Counterexamples in Group Theory

DESMOND MACHALE

University College

Cork, Ireland

In the theory of finite groups, many major theorems have been proved by the minimum counterexample technique which works as follows. If there is a counterexample to a given theorem, then there is a counterexample G of smallest possible order. The assumption that G exists is then used to force a contradiction and the theorem in question is thus established. In practice, the contradiction frequently arises from the existence of a counterexample of order smaller than that of the presumed minimum counterexample. This technique was used by G. A. Miller **[1]**, as early as 1916, though it may have been used by earlier writers. Of course, the minimum counterexample technique is merely a disguised form of mathematical induction and in fact bears the same kind of relation to induction as does proof by the method of infinite descent used in number theory.

However, even when a conjecture about finite groups turns out to be false, the question naturally arises as to which group furnishes us with a counterexample of smallest possible order. The search for counterexamples is an important aspect of the teaching of modern algebra, and the finding of minimum counterexamples, or "least criminals" as they are sometimes called, gives the student an excellent opportunity of becoming familiar with the groups of "small" order. Indeed, it is remarkable just how many conjectures can be refuted with a knowledge of the structures of the groups of order 12 or less.

In this paper we give a minimum counterexample for each of a number of not implausible conjectures about finite groups. Proofs can be found in standard references on group theory, but we have included a few arguments to illustrate the search technique. We also suggest many further problems, solved and perhaps unsolved, in this area. We work with groups given by generators and defining relations, or with groups given by their faithful permutation representations. We note that a minimum counterexample need not be unique since nonisomorphic minimum counterexamples (of the same order) may possibly exist for a given conjecture (as in Conjecture 1 below).

For handy reference throughout this note we list in TABLE 1 the notation which we shall use, and in TABLE 2 the groups of order less than 12.

G	a finite group
$Z(G)$	the center of G
G'	the commutator subgroup of G
$\lvert G\rvert$	the order of G
C_n	the cyclic group of order n
D_n	the dihedral group of order $2n$
A_n	the alternating group of order $n!/2$
Q	the quaternion group of order 8
$A\times B$	the direct product of A and B
F	the set $\{x^2 \mid x\in G\}$ of all squares in G
$G\simeq H$	the groups G and H are isomorphic
$H\lhd G$	H is a normal subgroup of G
$\operatorname{Aut} G$	the group of automorphisms of G
$\Phi(G)$	the Frattini subgroup of G (see [2])

TABLE 1

Order	Distinct nonisomorphic groups
1	C_1
2	C_2
3	C_3
4	$C_4, C_2\times C_2$
5	C_5
6	$C_6\simeq C_2\times C_3, S_3\simeq D_3$
7	C_7
8	$C_8, C_4\times C_2, C_2\times C_2\times C_2, D_4, Q$
9	$C_9, C_3\times C_3$
10	$C_{10}\simeq C_2\times C_5, D_5$
11	C_{11}

TABLE 2

We will use standard notation for generators and relations for a group. For example, $S_3=\langle a,b \mid a^3=b^2=1,\ bab=a^2\rangle$ denotes the fact that the symmetric group S_3 can be described as the group whose elements are products of two elements a, b subject to the conditions that a is of order 3, b is of order 2, and the triple product bab collapses to a^2. This "generators and relations" notation allows us to avoid the tedious use of multiplication tables.

CONJECTURE 1. *In any group G, the set F of all squares of elements of G is a subgroup of G.*

If G is Abelian and x^2, y^2 are elements of F, then $x^2y^2=(xy)^2$, so F is closed and clearly nonempty and thus a subgroup of G. This fact rules out as counterexamples all groups of order less than 12 with the possible exceptions of S_3, D_4, Q and D_5.

Now $S_3\simeq D_3=\langle a,b\mid a^3=b^2=1,\ bab=a^2\rangle$ and direct calculation shows that $F=\{1,a,a^2\}$ is a subgroup of S_3. Next, for $D_4=\langle a,b\mid a^4=b^2=1,\ bab=a^3\rangle$, $F=\{1,a^2\}$, which is a subgroup of D_4. Similarly, $Q=\langle a,b\mid a^4=1,\ a^2=b^2, b^{-1}ab=a^3\rangle$ giving $F=\{1,a^2\}$, which is a subgroup of Q. Finally, $D_5=\langle a,b\mid a^5=b^2=1,\ bab=a^4\rangle$ giving $F=\{1,a,a^2,a^3,a^4\}$, a subgroup of D_5.

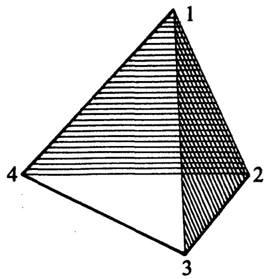


FIGURE 1. The rotation group of the regular tetrahedron permutes the vertices, and hence can be identified with A_4. This group is a minimum counterexample to several conjectures.

Thus a minimum counterexample has order at least 12, and we will now show that A_4, of order 12, is a minimum counterexample. Representing A_4 as a permutation group, we have

$$A_4=\{e,(12)(34),(13)(24),(14)(23),(123),(132),(124),(142),(134),(143),(234),(243)\}$$

(see FIGURE 1) and

$$F=\{e,(123),(132),(124),(142),(134),(143),(234),(243)\}.$$

So, since $|F|=9$, and 9 is not a divisor of $|A_4|$, F is not a subgroup of A_4. Note that the dicyclic group of order 12 given by $\langle a,b\,|\,a^6=1,\ b^2=a^3,\ b^{-1}ab=a^{-1}\rangle$ is also a minimum counterexample.

CONJECTURE 2. *The converse of Lagrange's theorem is true*; *i.e., if n divides* $|G|$, *then G has a subgroup of order n.*

Since it is known that the converse of Lagrange's theorem is true for all finite Abelian groups, we can rule out each group of order less than 12 as a minimum counterexample except possibly S_3, D_4, Q and D_5. For each of these groups we can produce subgroups of appropriate orders, in terms of the generators already given:

$$S_3:\{1\},\quad \{1,b\},\quad \{1,a,a^2\},\quad S_3.$$
$$D_4:\{1\},\quad \{1,a^2\},\quad \{1,a,a^2,a^3\},\quad D_4.$$
$$Q:\{1\},\quad \{1,a^2\},\quad \{1,a,a^2,a^3\},\quad Q.$$
$$D_5:\{1\},\quad \{1,b\},\quad \{1,a,a^2,a^3,a^4\},\quad D_5.$$

Hence none of these groups is a counterexample. However, A_4 is a minimum counterexample, since we can show that it has no subgroup of order 6. Direct calculation shows that the conjugacy classes in A_4 are

$$\{e\},\{(12)(34),(13)(24),(14)(23)\},\ \{(123),(134),(243),(142)\}$$

and

$$\{(132),(143),(234),(124)\}.$$

If H were a subgroup of order 6 in A_4, then, since $[A_4:H]=2, H\lhd A_4$. Therefore H must consist of complete conjugacy classes of A_4 and of course $e\in H$. The five nonidentity elements of H must be made up by taking complete classes with either 3 or 4 elements, an impossibility. Thus H cannot exist and so A_4 is a minimum counterexample.

CONJECTURE 3. *If A and B are subgroups of G such that* $B\lhd A$ *and* $A\lhd G$, *then* $B\lhd G$.

Since every subgroup of an Abelian group is normal, the only group of order less than 8 to be examined is S_3. Now $\{1\}\lhd\{1,a,a^2\}\lhd S_3$ is the only relevant normal chain in S_3, and since $\{1\}\lhd S_3, S_3$ does not produce a counterexample. However, D_4 of order 8 is a minimum counterexample, as we now prove. Since $D_4=\langle a,b\,|\,a^4=b^2=1,\ bab=a^3\rangle$, we take $B=\{1,b\}$,

$A=\{1, a^2, b, a^2b\}$. Then $B \lhd A$, since A is Abelian, and $A \lhd D_4$ since $[D_4: A]=2$, but clearly B is not normal in D_4 since $a^{-1}ba \notin B$.

CONJECTURE 4. *All groups of odd order are Abelian.*

This conjecture might be optimistically made on the strength of Feit and Thompson's remarkable result that all groups of odd order are soluble. We have the following well-known results:

(a) *Groups of order p or p^2 are Abelian, where p is a prime.*

(b) *If p and q are distinct primes with $p>q$ and if q does not divide $p-1$, then there is a unique group of order pq and this group is the Abelian group $C_{pq} \simeq C_p \times C_q$.*

These two results eliminate all groups of odd order less than 21 as counterexamples. However, there is a group G of order 21, given by $G=\langle a, b \mid a^7=b^3=1, b^{-1}ab=a^2\rangle$, and G is clearly nonAbelian, so G is the required minimum counterexample.

CONJECTURE 5. *$Z(G)$ is a fully invariant subgroup of G, i.e., $Z(G)$ is mapped into $Z(G)$ by every endomorphism of G.*

If G is Abelian or $Z(G)=\{1\}$, then $Z(G)$ is fully invariant, so all groups of order less than 12 are ruled out as counterexamples, except possibly D_4 and Q. In both of these groups it is easy to show that $Z(G)=G'$, so $Z(G)$ is fully invariant because it is known that G' is fully invariant. However, $D_6=\langle a, b \mid a^6=1=b^2, bab=a^5\rangle$ of order 12 is a minimum counterexample. In D_6 the mapping $a \to b$, $b \to b$, induces an endomorphism θ of D_6 such that $(a^3)\theta=b$, where $a^3 \in Z(D_6)$ and $b \notin Z(D_6)$.

CONJECTURE 6. *If $N \lhd G$, then G contains a subgroup isomorphic to the factor group G/N.*

This very natural conjecture is in fact true for finite Abelian groups, so S_3 is the only group of order less than 8 which needs to be considered. Now $\{1\}$, $\{1, a, a^2\}$, and S_3 are the normal subgroups of S_3, and the corresponding factor groups are isomorphic to S_3, C_2, and C_1. However, S_3 has subgroups isomorphic to each of these groups. But the quaternion group Q is a minimum counterexample. Let $Q=\langle a, b \mid a^4=1, a^2=b^2, b^{-1}ab=a^3\rangle$. Then $\langle a^2\rangle=A \lhd Q$ and $Q/A \simeq C_2 \times C_2$. However, Q has no subgroup isomorphic to $C_2 \times C_2$, since Q has only one element of order 2.

We close with a number of conjectures, all of which are **false**. The reader is challenged to produce a minimum counterexample in each case. At the time of writing, minimum counterexamples to those conjectures marked with an asterisk were unknown to the author. Some of these are likely to present considerable difficulty, and the author would welcome comments or solutions.

CONJECTURE 7. *In any group G, the set of all commutators forms a subgroup.*

CONJECTURE 8. *If every subgroup of G is normal, then G is Abelian.*

CONJECTURE 9. *If every proper subgroup of G is cyclic, then G is cyclic.*

CONJECTURE 10. *If every proper subgroup of G is cyclic, then G is Abelian.*

CONJECTURE 11. *If every proper subgroup of G is Abelian, then G is Abelian.*

CONJECTURE 12. *Every normal subgroup of G is characteristic in G.*

CONJECTURE 13. *Every characteristic subgroup is fully invariant in G.*

CONJECTURE 14. *Given a group G, there exists a group H such that $G \simeq H'$.*

CONJECTURE 15. *Given a group G, there exists a group H such that $G \simeq \text{Aut}\, H$.*

CONJECTURE 16. *Given a nonAbelian group G, there exists a finite group H such that* $G \simeq \operatorname{Aut} H$.

CONJECTURE 17. *Given a nonAbelian group G, there exists a finite group H such that* $G \simeq H/Z(H)$.

CONJECTURE 18. *Given a group G, there exists a finite group H such that* $G \simeq \Phi(H)$.

CONJECTURE 19. *Every group G has a subgroup of prime index.*

CONJECTURE 20. *If G is a simple group, then G is Abelian.*

CONJECTURE 21. *Every insoluble group G is simple.*

CONJECTURE 22. *If G is a group with trivial center, then* $G = G'$.

CONJECTURE 23. *If G is a group with $G = G'$, then G has trivial center.* (See [3], page 56.)

CONJECTURE 24. *If every group of order $|G|$ is cyclic, then $|G|$ must be a prime number (ignore* $|G| = 1$).

CONJECTURE 25*. *If an automorphism α of G sends every conjugacy class of G onto itself, then α must be inner.* (See [2], page 23.)

CONJECTURE 26*. *If G has a fixed-point-free automorphism, then G is nilpotent.* (See [3], page 336.)

CONJECTURE 27*. *If G is nonAbelian, then* $\operatorname{Aut} G$ *is nonAbelian.*

CONJECTURE 28*. *If G is nonAbelian, then* $|\operatorname{Aut} G|$ *is even, i.e., every nonAbelian group has an automorphism of order* 2.

CONJECTURE 29. *If G is nonAbelian, then G is a 2-generator group.*

CONJECTURE 30. *If G is a nonAbelian p-group, then* $\operatorname{Aut} G$ *cannot also be a p-group.*

CONJECTURE 31*. *If G is nonAbelian and $|G|$ is odd, then G has an outer automorphism.*

CONJECTURE 32. *If H is a proper subgroup of G, then* $|\operatorname{Aut} G| > |\operatorname{Aut} H|$. (See [2], page 24.)

CONJECTURE 33. *If $|G| = n > 1$, then there are less than n distinct isomorphism classes of groups of order n.*

CONJECTURE 34. *If G and H are groups such that G and H have exactly the same number of elements of each order, then* $G \simeq H$.

CONJECTURE 35. *If H is a normal nilpotent subgroup of G such that G/H is nilpotent, then G is nilpotent.*

CONJECTURE 36*. *If G is a nonAbelian p-group, where p is odd, then* $\operatorname{Aut} G$ *cannot also be a p-group.*

CONJECTURE 37. *The kernel of a Frobenius group G is Abelian.*

CONJECTURE 38. *If $|G| = |H|$ and* $\operatorname{Aut} G \simeq \operatorname{Aut} H$, *then* $G \simeq H$.

CONJECTURE 39. *If H is a subgroup of G, then* $\Phi(H) \subseteq \Phi(G)$. (See [2], page 50.)

CONJECTURE 40. *If $|G| = |H|$, and G and H have the same character table, then* $G \simeq H$.

CONJECTURE 41. *In any permutation group G, the product of transpositions, no two of which are equal, cannot be the identity element of G.*

CONJECTURE 42. *If A and B are subgroups of G such that $A \subset B \subset G$, where A is characteristic in G, then A is characteristic in B.*

CONJECTURE 43. *If G is a noncyclic group with* $|G| = n$, *then G can be faithfully embedded in* S_m *for some* $m < n$.

CONJECTURE 44. *If G is a nonAbelian group with* $|G| = n$, *then G can be faithfully embedded in* S_m *for some* $m < n$.

CONJECTURE 45. *Any element of* G' *is the product of at most two elements of F.*

CONJECTURE 46. *If A and B are normal subgroups of a group G such that* $A \simeq B$, *then* $G/A \simeq G/B$.

CONJECTURE 47. *If A and B are normal subgroups of a group G such that* $G/A \simeq G/B$, *then* $A \simeq B$.

References

[1] H. F. Blichfeldt, L. E. Dickson, and G. A. Miller, Theory and Applications of Finite Groups, Dover Reprint, New York, 1961.

[2] J. D. Dixon, Problems in Group Theory, Blaisdell, Waltham, Mass., 1967.

[3] D. Gorenstein, Finite Groups, Harper and Row, New York, 1968.

Regions of Convergence for a Generalized Lambert Series

DONALD H. TRAHAN
Naval Postgraduate School
Monterey, California 93940

In this note, we discuss infinite series of the form

$$G(z) = \Sigma \frac{a_n z^n}{1 + c_n z^n}$$

where the coefficients a_n and c_n are complex numbers and $c_n z^n \neq -1$. We will call this type of infinite series a **G-series**. A G-series is a power series if, for all n, $c_n = 0$ and a **Lambert series** if, for all n, $c_n = -1$.

In the literature a G-series is usually considered as a generalized Lambert series. For our investigation it might be better to think of a Lambert series as a generalized power series since the questions we will consider can be readily understood in terms of what is known about power series. For example, we inquire—does a G-series have a radius of convergence? Are there convergence criteria for G-series similar to well-known criteria of power series?

We first consider Lambert series. In general, a Lambert series is analytic at the origin and therefore has a power series expansion at the origin. Some of these power series expansions are very interesting. For example, J. H. Lambert found that for $|z| < 1$

$$\sum_{n=1}^{\infty} \frac{z^n}{1 - z^n} = \sum_{n=1}^{\infty} \tau_n z^n = z + 2z^2 + 2z^3 + 3z^4 + 2z^5 + 4z^6 + \cdots,$$

where τ_n is the number of divisors of n. More generally, provided r is a real number and $|z| < 1$, CONJECTURE 43. *If G is a noncyclic group with $|G| = n$, then G can be faithfully embedded in S_m for some $m < n$.*

CONJECTURE 44. *If G is a nonAbelian group with $|G| = n$, then G can be faithfully embedded in S_m for some $m < n$.*

CONJECTURE 45. *Any element of G' is the product of at most two elements of F.*

CONJECTURE 46. *If A and B are normal subgroups of a group G such that $A \simeq B$, then $G/A \simeq G/B$.*

CONJECTURE 47. *If A and B are normal subgroups of a group G such that $G/A \simeq G/B$, then $A \simeq B$.*

References

[1] H. F. Blichfeldt, L. E. Dickson, and G. A. Miller, Theory and Applications of Finite Groups, Dover Reprint, New York, 1961.

[2] J. D. Dixon, Problems in Group Theory, Blaisdell, Waltham, Mass., 1967.

[3] D. Gorenstein, Finite Groups, Harper and Row, New York, 1968.

Regions of Convergence for a Generalized Lambert Series

DONALD H. TRAHAN
Naval Postgraduate School
Monterey, California 93940

In this note, we discuss infinite series of the form

$$G(z) = \Sigma \frac{a_n z^n}{1 + c_n z^n}$$

where the coefficients a_n and c_n are complex numbers and $c_n z^n \neq -1$. We will call this type of infinite series a **G-series**. A G-series is a power series if, for all $n, c_n = 0$ and a **Lambert series** if, for all $n, c_n = -1$.

In the literature a G-series is usually considered as a generalized Lambert series. For our investigation it might be better to think of a Lambert series as a generalized power series since the questions we will consider can be readily understood in terms of what is known about power series. For example, we inquire—does a G-series have a radius of convergence? Are there convergence criteria for G-series similar to well-known criteria of power series?

We first consider Lambert series. In general, a Lambert series is analytic at the origin and therefore has a power series expansion at the origin. Some of these power series expansions are very interesting. For example, J. H. Lambert found that for $|z| < 1$

$$\sum_{n=1}^{\infty} \frac{z^n}{1 - z^n} = \sum_{n=1}^{\infty} \tau_n z^n = z + 2z^2 + 2z^3 + 3z^4 + 2z^5 + 4z^6 + \cdots,$$

where τ_n is the number of divisors of n. More generally, provided r is a real number and $|z| < 1$, then

$$\sum_{n=1}^{\infty} \frac{n^r z^n}{1-z^n} = \sum_{n=1}^{\infty} \tau_n^r z^n,$$

where τ_n^r is the sum of the rth powers of all divisors of n and $\tau_n^0 = \tau_n$. One of the most important studies of Lambert series is Konrad Knopp's paper [3] of 1913.

In 1932, J. M. Feld [2] established that a function $f(z)$ which is analytic at the origin has a G-series expansion

$$f(z) = b_0 + \sum_{n=1}^{\infty} \frac{a_n b_n z^n}{1 - a_n z^n}$$

in some region about the origin. In this preceding series the terms b_n are preassigned constants, although they are required to satisfy some restrictions. In 1939, William Doyle [1] studied the region of convergence for an infinite series of the form

$$\sum \frac{a_n b_n z^{\lambda n}}{1 - a_n z^{\mu n}},$$

where λ is any integer and μ is a positive integer. Doyle's study is not complete; we will raise some questions about G-series that are not considered in his paper.

We first note two theorems (A and B) which give convergence criteria for G-series. Although the results are essentially due to Doyle, we give an explicit formula for the radius of the circle of convergence. Given a G-series

$$\sum \frac{a_n z^n}{1 + c_n z^n},$$

define α, $\underline{\alpha}$, γ, and $\underline{\gamma}$ as follows:

$$1/\alpha = \overline{\lim} \sqrt[n]{|a_n|}, \qquad 1/\gamma = \overline{\lim} \sqrt[n]{|c_n|},$$

$$1/\underline{\alpha} = \underline{\lim} \sqrt[n]{|a_n|}, \quad \text{and} \quad 1/\underline{\gamma} = \underline{\lim} \sqrt[n]{|c_n|}.$$

THEOREM A. *If* $|z| < \gamma$, *then the G-series* $\sum \frac{a_n z^n}{1 + c_n z^n}$ *converges if and only if the power series* $\sum a_n z^n$ *converges.*

THEOREM B. *If* $|z| > \underline{\gamma}$ *and* $c_n \neq 0$, *then the G-series* $\sum \frac{a_n z^n}{1 + c_n z^n}$ *converges if and only if the series* $\sum \frac{a_n}{c_n}$ *converges.*

Using a technique employed by Knopp in [3] and [4], Doyle established these results [1] using a well-known theorem by du Bois-Reymond. We will use only elementary ideas from complex analysis to establish our results on convergence criteria, and Theorems A and B follow from our work. The following lemmas will be useful in the proofs of our theorems.

LEMMA 1. *If* $|z| > \underline{\alpha}$, *and* $a_n \neq 0$ *for all* n, *then the power series* $\sum \frac{1}{a_n} z^{-n}$ *converges absolutely.*

Proof. Let $b_n = \sqrt[n]{|a_n|}$. Since $\overline{\lim} \frac{1}{b_n} = \frac{1}{\underline{\lim} b_n}$, the power series converges for $|z^{-1}| < \underline{\lim} \sqrt[n]{|a_n|}$ and hence for $|z| > \underline{\alpha}$.

LEMMA 2. *Assume the infinite series* $\sum \varepsilon_n$ *converges absolutely. The series* $\sum a_n(1-\varepsilon_n)$ *converges (absolutely) if and only if the series* $\sum a_n$ *converges (absolutely).*

Proof. If the series Σa_n converges (absolutely), then the series $\Sigma a_n(1-\varepsilon_n)$ converges (absolutely) since the second series can be expressed as the difference of two (absolutely) convergent series. Suppose the series Σa_n diverges. If $\lim a_n=0$, then $\Sigma a_n\varepsilon_n$ converges and hence $\Sigma a_n(1-\varepsilon_n)$ diverges by contradiction. On the other hand, if $\{a_n\}$ is not a null sequence, then $\{a_n(1-\varepsilon_n)\}$ is not a null sequence. Thus, in either case the series $\Sigma a_n(1-\varepsilon_n)$ diverges.

We can now prove our first theorem, which gives a complete solution to the problem of finding the radius of convergence of a G-series, provided $\alpha<\gamma$.

THEOREM 1. *Assume $\alpha<\gamma$. The G-series $\Sigma \dfrac{a_n z^n}{1+c_n z^n}$*

(i) *converges absolutely for $|z|<\alpha$,*
(ii) *converges or diverges with $\Sigma a_n z^n$ for $|z|=\alpha$, and*
(iii) *diverges for $|z|>\alpha$.*

Proof. If $|z|\leqslant\alpha$, then $|z|<\gamma$ and the infinite series $\Sigma c_n z^n/(1+c_n z^n)$ converges absolutely. We can rewrite the G-series as

$$G(z)=\Sigma a_n z^n\left[1-\frac{c_n z^n}{1+c_n z^n}\right].$$

Lemma 2 now implies conclusions (i) and (ii) of the theorem. (Note Lemma 2 also implies that the G-series diverges in the annular ring $\alpha<|z|<\gamma$.)

To prove (iii), assume $|z|>\alpha$. There is a subsequence $\{|a_{n_k}|^{1/n_k}\}$ of $\{|a_n|^{1/n}\}$ which converges to $\alpha^{-1}, \alpha>0$. Since $|z|>\alpha$, it follows that $|a_{n_k}z^{n_k}|\to\infty$. Therefore, the G-series diverges unless $|c_{n_k}z^{n_k}|\to\infty$. If $|c_{n_k}z^{n_k}|\to\infty$, then we proceed as follows. Since $\alpha<\gamma$, then for k sufficiently large $|a_{n_k}|>|c_{n_k}|$. From the identity

$$\frac{a_n z^n}{1+c_n z^n}=\frac{a_n}{c_n}\,\frac{1}{1+\dfrac{1}{c_n}z^{-n}}$$

it follows that the general term of the G-series does not approach zero, and therefore the series diverges.

Note that Theorem A is implied by (i) and (ii) of Theorem 1.

It is reasonable to inquire whether there is a theorem which is similar to Theorem 1 for the cases $\alpha=\gamma$ or $\alpha>\gamma$. For $\alpha>\gamma$, we will later show (Examples 1 and 2) that the answer to this question is negative. For G-series with $\alpha\geqslant\gamma$, we will use a different approach. Instead of a single theorem, we give several tests that can be used to analyze G-series in this case. The following theorem generalizes part (i) of Theorem 1.

THEOREM 2. *Assume $|z|<\alpha$. If there is no subsequence of $\{c_n z^n\}$ which has limit -1, then the G-series $\Sigma \dfrac{a_n z^n}{1+c_n z^n}$ converges absolutely.*

The next theorem is an improvement on Theorem B.

THEOREM 3. *If $|z|>\gamma$ and $c_n\neq 0$ for all n, then the G-series $\Sigma a_n z^n/(1+c_n z^n)$ converges (absolutely) if and only if the series $\Sigma a_n/c_n$ converges (absolutely).*

Proof. Consider the general term of the G-series

$$\frac{a_n z^n}{1+c_n z^n}=\frac{a_n}{c_n}\left[1-\frac{c_n^{-1}z^{-n}}{1+c_n^{-1}z^{-n}}\right].$$

By Lemma 1 the series $\Sigma c_n^{-1}z^{-n}$ converges absolutely, hence the result follows from Lemma 2.

A well-known convergence criterion for alternating series due to Leibnitz states that if $a_n > 0$, $a_n \geqslant a_{n+1}$ for all n, and $\lim a_n = 0$, then $\Sigma(-1)^n a_n$ converges. We can now generalize this result to apply to G-series.

COROLLARY. *If $a_n > 0$, $a_n \geqslant a_{n+1}$ for all n, and $\lim a_n = 0$, then for $|z| \neq 1$ the series*

$$\Sigma \frac{a_n z^n}{1+(-1)^n z^n}$$

converges. In addition, for $|z| < \alpha$, $|z| \neq 1$, the series converges absolutely.

Proof. By Leibnitz's theorem the power series $\Sigma a_n z^n$ converges for $z = -1$. Hence $\alpha \geqslant 1$. The result follows from Theorems 2 and 3.

THEOREM 4. (i) *Let $|z| > \underline{\alpha}$ and $a_n \neq 0$, $c_n \neq 0$ for all n. If $\{a_n/c_n\}$ is not a null sequence, then the G-series $\Sigma a_n z^n/(1+c_n z^n)$ diverges.*

(ii) *Let $|z| > \underline{\alpha}$, $a_n \neq 0$, $c_n \neq 0$ for all n. The G-series $\Sigma a_n z^n/(1+c_n z^n)$ converges absolutely if and only if the series $\Sigma a_n/c_n$ converges absolutely.*

Proof. Each of these two results follows from Lemma 1 and by writing the G-series in the form

$$\Sigma \frac{1}{a_n^{-1} z^{-n} + \dfrac{c_n}{a_n}}.$$

COROLLARY. *If $\underline{\alpha} < \underline{\gamma}$ and $|z| > \underline{\alpha}$, then the G-series $\Sigma a_n z^n/(1+c_n z^n)$ diverges.*

Proof. As in the proof of Theorem 1 part (iii), it follows that $\{a_n/c_n\}$ is not a null sequence. The result follows by Theorem 4 (i).

We now apply some of these results to G-series in which $\alpha > \gamma$. In the first example, the radius of convergence of the G-series is α, and in the second example, the radius of convergence is $\underline{\alpha}$. This shows that the conclusions in Theorem 1 do not hold in general when $\alpha > \gamma$.

EXAMPLE 1. Consider the G-series $\Sigma a_n z^n/(1+c_n z^n)$ where $a_{2n} = 2^{-2n}$, $a_{2n+1} = 3^{-(2n+1)}$, $c_{2n} = 4^{-2n}$, and $c_{2n+1} = 1$. We first determine that $\alpha = 2$, $\underline{\alpha} = 3$, $\gamma = 1$, and $\underline{\gamma} = 4$. By the Corollary to Theorem 4 the G-series diverges for $|z| > 3$. For $2 \leqslant |z| \leqslant 4$, the series diverges since $\{|a_{2n} z^{2n}|\}$ approaches one or infinity and $|1 + c_{2n} z^{2n}| \leqslant 2$. If $|z| < 2$ and $|z| \neq 1$, then by Theorem 2 the series converges absolutely. Therefore, the radius of convergence of this infinite series is $\alpha = 2$.

EXAMPLE 2. Consider the G-series $\Sigma a_n z^n/(1+c_n z^n)$ such that $a_{2n} = 3^{-2n}$, $a_{2n+1} = 2^{-(2n+1)}$, $c_{2n} = 4^{-2n}$, and $c_{2n+1} = 1$. For this series $\alpha = 2$, $\underline{\alpha} = 3$, $\gamma = 1$, and $\underline{\gamma} = 4$. By the Corollary to Theorem 4 the given series diverges for $|z| > 3$. If $|z| < 2$ and $|z| \neq 1$, then by Theorem 2 the series converges absolutely. In addition, for $2 \leqslant |z| < 3$ the series converges absolutely, since both the series of the even terms and the series of the odd terms of the given series converge absolutely. Therefore, in this example, the radius of convergence of the infinite series is $\underline{\alpha} = 3$.

For a power series, the circle of convergence and the circle of absolute convergence have the same radius. Our next example shows that this is not always true for a G-series.

EXAMPLE 3. Consider the series $\Sigma(-1)^n z^n/(1+nz^n)$. By Theorem 2, the series converges absolutely for $|z| < 1$. By Theorem 3 the series converges conditionally for $|z| > 1$. By working with the series itself, one can show the series does not converge absolutely for $|z| = 1$.

There are some problems about the regions of convergence and absolute convergence of a G-series that may be worth additional study. From our point of view, we consider only points in the complex plane such that $c_n z^n \neq -1$. We wonder—if $\alpha = \gamma$ or $\alpha > \gamma$, does a G-series have a circle of convergence? This question has two interpretations. We can consider the question if we include all points z such that $c_n z^n \neq -1$. On the other hand, it may be worthwhile to consider the radius of convergence of a G-series, but exclude points on certain circles in the complex plane. Specifically, let L be the set of all limit points of $|c_n|^{-1/n}$, then γ and $\bar{\gamma}$ are in L. We now ask—if $|z| \neq l$, $l \in L$, and $c_n z^n \neq -1$, does a G-series have a circle of convergence?

References

[1] William Doyle, A generalized Lambert series and its Moebius function, Ann. of Math., 40, #2 (1939) 353–359.

[2] J. M. Feld, The expansion of analytic functions in generalized Lambert series, Ann. of Math., 33 (1932) 139–142.

[3] Konrad Knopp, Ueber Lambertsche Reinhen, Journal für Math., 142 (1913) 283–315.

[4] Konrad Knopp, Theory and Application of Infinite Series, Blackie and Sons, London, 1946, pp. 448–452.

Mersenne Numbers and Binomial Coefficients

RADE M. DACIĆ

Institut Mathématique

Belgrade, Yugoslavia

If you had a large Pascal's triangle of binomial coefficients, you might notice that all of the entries in rows 1, 3, 7, 15, 31, 63,... (these numbers of the form $2^n - 1$ are called Mersenne numbers) are odd integers and each of the other rows had at least one even entry. This may be well known: it is the purpose of this note to give a proof which may be less well known and which can be understood without very much training in number theory.

THEOREM. *$\binom{n}{k}$ is odd for all k, $k = 0, 1 \ldots, n$, if and only if $n = 2^s - 1$ for some s, $s = 1, 2 \ldots$.*

Proof. If $n = 2^s - 1$, then

$$\binom{n}{k} = \frac{2^s - 1}{1} \cdot \frac{2^s - 2}{2} \cdots \frac{2^s - k}{k}. \tag{1}$$

If $0 \leqslant k \leqslant n$, then $k = 2^u v$, where $0 \leqslant u \leqslant s$ and v is odd. So, cancelling a 2^u, $(2^s - k)/k = (2^{s-u} - v)/v$, which is a quotient of two odd integers. Thus, after cancellation, the right-hand side of (1) consists only of odd integers and hence $\binom{n}{k}$ is odd.

To prove the converse, suppose that n is odd and $2^{m-1} < n < 2^m$. Then $n = 2^{m-1} + 2p + 1$, where $0 \leqslant p \leqslant 2^{m-2} - 3$. Let $k = 2p + 2$. Then

$$\binom{n}{k} = \binom{n}{k-1} \cdot \frac{n-k+1}{k} = s \cdot \frac{2^{m-1}}{2p+2} = s \cdot \frac{2^{m-2}}{p+1},$$

where s is an integer. Since $p + 1 < 2^{m-2}$, not all of the twos can be cancelled and $\binom{n}{k}$ is even. If n is even, then $\binom{n}{1}$ is even, and this completes the proof.

There are some problems about the regions of convergence and absolute convergence of a G-series that may be worth additional study. From our point of view, we consider only points in the complex plane such that $c_n z^n \neq -1$. We wonder—if $\alpha = \gamma$ or $\alpha > \gamma$, does a G-series have a circle of convergence? This question has two interpretations. We can consider the question if we include all points z such that $c_n z^n \neq -1$. On the other hand, it may be worthwhile to consider the radius of convergence of a G-series, but exclude points on certain circles in the complex plane. Specifically, let L be the set of all limit points of $|c_n|^{-1/n}$, then $\underline{\gamma}$ and $\bar{\gamma}$ are in L. We now ask—if $|z| \neq l$, $l \in L$, and $c_n z^n \neq -1$, does a G-series have a circle of convergence?

References

[1] William Doyle, A generalized Lambert series and its Moebius function, Ann. of Math., 40, #2 (1939) 353–359.

[2] J. M. Feld, The expansion of analytic functions in generalized Lambert series, Ann. of Math., 33 (1932) 139–142.

[3] Konrad Knopp, Ueber Lambertsche Reinhen, Journal für Math., 142 (1913) 283–315.

[4] Konrad Knopp, Theory and Application of Infinite Series, Blackie and Sons, London, 1946, pp. 448–452.

Mersenne Numbers and Binomial Coefficients

Rade M. Dacić

Institut Mathématique

Belgrade, Yugoslavia

If you had a large Pascal's triangle of binomial coefficients, you might notice that all of the entries in rows 1, 3, 7, 15, 31, 63,... (these numbers of the form $2^n - 1$ are called Mersenne numbers) are odd integers and each of the other rows had at least one even entry. This may be well known: it is the purpose of this note to give a proof which may be less well known and which can be understood without very much training in number theory.

THEOREM. *$\binom{n}{k}$ is odd for all k, $k = 0, 1 \ldots, n$, if and only if $n = 2^s - 1$ for some s, $s = 1, 2 \ldots$.*

Proof. If $n = 2^s - 1$, then

$$\binom{n}{k} = \frac{2^s - 1}{1} \cdot \frac{2^s - 2}{2} \cdots \frac{2^s - k}{k}. \tag{1}$$

If $0 \leqslant k \leqslant n$, then $k = 2^u v$, where $0 \leqslant u \leqslant s$ and v is odd. So, cancelling a 2^u, $(2^s - k)/k = (2^{s-u} - v)/v$, which is a quotient of two odd integers. Thus, after cancellation, the right-hand side of (1) consists only of odd integers and hence $\binom{n}{k}$ is odd.

To prove the converse, suppose that n is odd and $2^{m-1} < n < 2^m$. Then $n = 2^{m-1} + 2p + 1$, where $0 \leqslant p \leqslant 2^{m-2} - 3$. Let $k = 2p + 2$. Then

$$\binom{n}{k} = \binom{n}{k-1} \cdot \frac{n-k+1}{k} = s \cdot \frac{2^{m-1}}{2p+2} = s \cdot \frac{2^{m-2}}{p+1},$$

where s is an integer. Since $p + 1 < 2^{m-2}$, not all of the twos can be cancelled and $\binom{n}{k}$ is even. If n is even, then $\binom{n}{1}$ is even, and this completes the proof.

Calculations for Bertrand's Postulate

HEIKO HARBORTH
ARNFRIED KEMNITZ
Technische Universität
D-3300 Braunschweig
West Germany

In 1845 J. Bertrand conjectured in **[1]** that for all $n>6$, there is at least one prime between $n/2$ and $n-2$. Actually, Euler had already formulated this conjecture nearly a hundred years earlier (see **[9]**). He used the form which now is well known as Bertrand's postulate, $\pi(2n)-\pi(n)>0$ for all $n\geqslant 1$, where $\pi(n)$ denotes the number of primes less than or equal to n. The first proof was given by Tchebychev in **[15]**, 369–382. Moreover, Tchebychev proved the following extension of Bertrand's postulate for $\varepsilon_0=1/5$: For any $\varepsilon>\varepsilon_0\geqslant 0$, there exists an $n(\varepsilon)$ so that for all $n\geqslant n(\varepsilon)$,

$$\pi((1+\varepsilon)n)-\pi(n)>0.$$

In 1896 the first proof of the famous prime number theorem guaranteed that $\varepsilon_0=0$. However, it is impossible to infer from this proof exact values for the smallest $n(\varepsilon)$; we shall denote this smallest value by $n_0(\varepsilon)$. Several authors, using Tchebychev's elementary methods, have determined some specific values for $n_0(\varepsilon)$. The best value so far obtained by elementary methods, $n_0(1/13)=118$, can be found in **[10]**, along with extensive references. In **[11]**, **[12]**, and **[13]** Rosser and Schoenfeld used heavy computations and complex variable theory to determine $n_0(\varepsilon)=2{,}010{,}760$ for $\varepsilon=1/16597$.

For the proofs of many problems in elementary number theory (e.g., **[2]**–**[8]**) it is useful to have prepared more special pairs ε and $n_0(\varepsilon)$.

It is the purpose of this note to present tables which enable a certain choice for problem solvers, and for any use of these generalizations of Bertrand's postulate.

We used the results of Rosser and Schoenfeld, a modified prime number generator of Singleton **[14]**, and the computer ICL 1906 S of the Technical University Braunschweig to generate TABLES 1–3. The last value of TABLE 1 corresponds to $\varepsilon=1/17172$, which is somewhat smaller than the above cited value. For this result we used the private communication of R. P. Brent that the difference of consecutive primes is smaller than 653 up to $4.444\cdot 10^{12}$.

ε	$n_0(\varepsilon)$	ε	$n_0(\varepsilon)$	ε	$n_0(\varepsilon)$
1	1	0.003	9978	0.0004	188032
0.5	8	0.002	31407	0.0003	370262
0.2	25	0.001	48683	0.0002	492129
0.1	116	0.0009	58837	0.0001	860153
0.05	213	0.0008	60541	0.00009	1357211
0.02	1335	0.0007	89691	0.00008	1561927
0.01	2479	0.0006	89700	0.00007	2010741
0.005	5751	0.0005	155930	0.00006	2010761
				0.000058231	2010764

The smallest $n_0(\varepsilon)$ with $\pi((1+\varepsilon)n)-\pi(n)>0$ for all $n\geqslant n_0(\varepsilon)$.

TABLE 1

n_0	$\varepsilon(n_0)$	n_0	$\varepsilon(n_0)$	n_0	$\varepsilon(n_0)$
5	0.571429	250	0.047782	5000	0.005724
10	0.307693	300	0.044165	8000	0.004016
20	0.260870	400	0.034417	10000	0.002964
30	0.193549	500	0.034417	14000	0.002806
50	0.127660	800	0.025622	20000	0.002294
100	0.123894	1000	0.025622	30000	0.002294
140	0.064286	2000	0.011015	50000	0.000986
200	0.056873	3000	0.008561	80000	0.000714

The smallest $\varepsilon=\varepsilon(n_0)$ (up to 6 decimals) with $\pi((1+\varepsilon)n)-\pi(n)>0$ for all $n \geqslant n_0$.

TABLE 2

ε \ m	1	2	3	4	5	10	15	20
1	1	6	9	15	21	49	76	115
0.5	8	20	25	32	48	116	168	245
0.1	116	203	207	318	321	776	1320	1794
0.05	213	321	531	771	1333	1893	3013	3365
0.01	2479	4160	5584	6483	7378	14180	18843	27136
0.005	5751	9554	11184	18805	19584	35623	44298	58604
0.001	48683	62235	83120	107474	121732	227750	295464	406743

The smallest $n_0(\varepsilon, m)$ with $\pi((1+\varepsilon)n)-\pi(n) \geqslant m$ for all $n \geqslant n_0(\varepsilon, m)$.

TABLE 3

This note is dedicated to Professor Dr. Hans-Joachim Kanold on the occasion of his 65th birthday.

References

[1] J. Bertrand, Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme, J. de l'École Polytechnique, 18 (1845) 123–140.

[2] D. M. Bloom, Problem E 2157, Amer. Math. Monthly, 76 (1969) 1144.

[3] P. Erdős, Aufgabe 748, Elem. Math., 31 (1976) 98.

[4] P. Erdős, A property of 70, this MAGAZINE, 51 (1978) 238–240.

[5] E. Härtter, Aufgabe 719, Elem. Math., 30 (1975) 60–61.

[6] H. Harborth, Eine Eigenschaft aufeinanderfolgender Zahlen, Arch. Math. (Basel), 21 (1970) 50–51.

[7] E. Just and N. Schaumberger, Problem 6194, Amer. Math. Monthly, 85 (1978) 122.

[8] R. S. Luthar, Problem E 2078, Amer. Math. Monthly, 76 (1969) 416.

[9] G. N. Matwiewskaja, Das Bertrandsche Postulat in Eulers Aufzeichnungen (Russian), Istor.-Mat. Issled., 14 (1961) 285–288.

[10] H. Rohrbach and J. Weis, Zum finiten Fall des Bertrandschen Postulats, J. Reine Angew. Math., 214/215 (1964) 432–440.

[11] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math., 6 (1962) 64–94.

[12] J. B. Rosser and L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, Math. Comp., 29 (1975) 243–269.

[13] L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, II, Math. Comp., 30 (1976) 337–360.

[14] R. C. Singleton, An efficient prime number generator, Comm. ACM, 12 (1969) 563–564.

[15] P. L. Tchebychev, Mémoire sur les nombres premiers, J. Math. Pures Appl. (1), 17 (1852) 366–390.

PROBLEMS

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

Proposals

To be considered for publication, solutions should be mailed before July 1, 1981.

1112. The function $\sin(1/t)$ is bounded and continuous everywhere except at 0, thus is (Riemann) integrable over any bounded interval. We may, therefore, define $F(x)$ to be $\int_0^x \sin(1/t)\,dt$, where x is any real number. Is F differentiable at 0? [*Richard Dowds, Fredonia State University College.*]

1113. On Christmas Eve, 1983, Dean Jixon, the famous seer who had made startling predictions of the events of the preceding year, declared that the volcanic and seismic activities of 1980 and 1981 were connected with mathematics. The diminishing of this geologic activity depended upon the existence of an elementary proof of the irreducibility of the polynomial $P(x)=x^{1981}+x^{1980}+12x^2+24x+1983$. Is there such a proof? [*William A. McWorter, Jr., The Ohio State University.*]

1114. Prove or disprove: There exists a function f defined on $[-1,1]$ with f' continuous such that $\sum_{n=1}^{\infty} f(1/n)$ converges but $\sum_{n=1}^{\infty}|f(1/n)|$ diverges. (This is a relaxing of the condition "f'' continuous" to "f' continuous" in Problem 1060, this MAGAZINE, January 1979 and March 1980.) [*Robert Clark, student, Temple University.*]

1115. Let D be the disc $x^2+y^2<1$. Let points A and B be selected at random in D. Find the probability that the open disc whose center is the midpoint of $\overline{AB}$ and whose radius is $AB/2$ is a subset of D. [*Roger L. Creech, East Carolina University.*]

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 acknowledgment 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

Pythagorean Triangles — November 1979

1088. (a) For each positive integer m, how many Pythagorean triangles are there which have an area equal to m times the perimeter? How many of these are primitive?

(b*) Can this result be generalized to all triangles with integer sides and area equal to m times the perimeter? [*Alan Wayne, Pasco-Hernando Community College.*]

Solution (a): It is well known that the legs of a Pythagorean triangle are $2kuv$ and $k(u^2-v^2)$, and the hypotenuse is $k(u^2+v^2)$, for some integers k, u and v, and that this representation is unique provided $k>0$, $u>v>0$, and u and v are relatively prime and not both odd. Setting the area equal to m times the perimeter yields $kv(u-v)=2m$.

Consider first the number a_m of primitive ($k=1$) Pythagorean triangles corresponding to a fixed ratio m. Because u and v have opposite parity, $u-v$ is odd. Because u and v are relatively prime, so are v and $u-v$. If $m=2^{k_0}p_1^{k_1}\cdots p_r^{k_r}$ is the canonical factorization of m (where possibly $k_0=0$), any power 2^{k_0} (and the additional factor of 2) must divide v, while each of the r powers $p_i^{k_i}$ must divide either v or else $u-v$. Hence $a_m=2^r$.

Consider next the number b_m of all Pythagorean triples corresponding to a fixed ratio m. In the equation $kv(u-v)=2m$, k and v can contribute the k_0+1 factors of 2 in $2m$ in k_0+2 ways. For each $i=1,2,\ldots,r$: either k can contribute all k_i factors of p_i; or v can contribute some, and k the others, in k_i ways; or else $u-v$ can contribute some, and k the others, in k_i ways. Hence $b_m=(k_0+2)(2k_1+1)\cdots(2k_r+1)$.

ROBERT PATENAUDE
California State College, Bakersfield

Part (a) also solved by Bern Problem Solving Group (Switzerland), Walter Bluger (Canada), P. J. Federico, Steven Kleiman & Henry Klostergaard, L. Kuipers (Switzerland), Scott Smith, Lawrence Somer, Dave Van Leeuwen, Michael Vowe (Switzerland), Ken Yocum, and the proposer. Federico gave a discussion of the equations which must be satisfied to solve part (b). Kleiman & Klostergaard have written an article for publication which discusses an algorithm for solving part (b).

Old Year Resolution — January 1980

1089. Determine the highest power of 1980 which divides

$$\frac{(1980n)!}{(n!)^{1980}}.$$

[*M. S. Klamkin, University of Alberta.*]

Solution: Let $V_m(x)$ be the exponent of the highest power of m which divides x. If p is a prime,

$$V_p\left(\frac{(mn)!}{(n!)^m}\right)=V_p((mn)!)-mV_p(n!)=\sum_{k>1}\left(\left[\frac{mn}{p^k}\right]-m\left[\frac{n}{p^k}\right]\right).$$

Thus, if m has the prime factorization $m=\prod_{i=1}^r p_i^{e_i}$,

$$V_m\left(\frac{(mn)!}{(n!)^m}\right)=\min_i\left[\frac{1}{e_i}\sum_{k>1}\left(\left[\frac{mn}{p_i^k}\right]-m\left[\frac{n}{p_i^k}\right]\right)\right].$$

The brackets $[\cdot]$ in all cases denote the greatest integer, and we note that the summand is the m-residue of $[mn/p_i^k]$. In particular, since $1980=2^2 3^2 \cdot 5 \cdot 11$,

$$V_{1980}\left(\frac{(1980n)!}{(n!)^{1980}}\right)=\min_{1\leqslant i\leqslant 4}\left[\frac{1}{e_i}\sum_{k\geqslant 1}\left(\left[\frac{1980n}{p_i^k}\right]-1980\left[\frac{n}{p_i^k}\right]\right)\right],$$

where $e_1=e_2=2$, $e_3=e_4=1$, and p_1, p_2, p_3 and p_4 are 2, 3, 5 and 11, respectively. Depending upon n, the minimum may occur in any of the four terms. $V_p((mn)!/(n!)^m)$ is small when n is a power of p, and for $p^{k-1}\leqslant n<p^k$, it grows with the sum of the digits of n in base p. If $n=8$, the minimum in V_{1980} occurs when $p=2$; if $n=9$, 5 or 11, it occurs when $p=3$, 5 or 11 respectively.

G. A. HEUER
Concordia College
&
KARL HEUER
Moorhead, Minnesota

Also solved by William E. Gould and the proposer. Klamkin also shows that when p is a prime the relative maximum values of $V_p((pn)!/(n!)^p)$ as a function of n occur when $n=p^m-1$ and the value then is $m(p-1)$.

A GCD Problem **January 1980**

1090. It is well known that if n is prime, then for every pair of relatively prime integers a and b the gcd of $(a^n-b^n)/(a-b)$ and $(a-b)$ is 1 or n. Find a corresponding result valid for every integer $n\geqslant 1$ and every pair of distinct integers a and b. [*Tom M. Apostol, California Institute of Technology*.]

Solution: Let (x,y) denote the gcd of x and y. We will prove the general formula

$$\left(\frac{a^n-b^n}{a-b},a-b\right)=\left(n(a,b)^{n-1},a-b\right).$$

When $(a,b)=1$ the right member is $(n,a-b)$, and when n is prime this is 1 or n.

We use the identity

$$\frac{a^n-b^n}{a-b}=\sum_{k=0}^{n-1}a^k b^{n-1-k}=\sum_{k=1}^{n-1}(a^k-b^k)b^{n-1-k}+nb^{n-1}$$
$$=(a-b)Q(a,b)+nb^{n-1}, \qquad (1)$$

where $Q(a,b)$ is a polynomial in a and b with integer coefficients.

Let

$$d=\left(\frac{a^n-b^n}{a-b},a-b\right),\quad e=\left(n(a,b)^{n-1},a-b\right).$$

From (1) we see that $d|nb^{n-1}$. By symmetry, $d|na^{n-1}$ so $d|n(a^{n-1},b^{n-1})=n(a,b)^{n-1}$, hence $d|e$. Also $e|nb^{n-1}$ and $e|(a-b)$ and (1) shows that $e|(a^n-b^n)/(a-b)$, hence $e|d$, so $e=d$.

TOM M. APOSTOL
California Institute of Technology

Also solved by Gordon Fisher, L. Kuipers (Switzerland), Lawrence Somer, and Ken Yocom.

REVIEWS

Paul J. Campbell, Editor
Beloit College

Pierre J. Malraison, Jr., Editor
MDSI, Ann Arbor

Assistant Editor: Eric S. Rosenthal, West Orange, NJ. Articles and books are selected for this section to call attention to interesting mathematical exposition that occurs outside the mainstream of the mathematics literature. Readers are invited to suggest items for review to the editors.

Mathematics Calendar 1981, Springer-Verlag, 1980; 26 pp, $12.95 (P).

Text and illustrations on Arrow's paradox, soap films, knots, computer chess, Dirichlet domains in crystallography, symmetry in art, Edgeworth on averages, the probabilistic abacus, self inverse fractals, an ancient Greek analog computer, strange attractors, and computerized tomography.

Newell, Virginia K., *et.al.*, Black Mathematicians and Their Works, Dorrance, 1980; xvi + 327 pp, $12.50 (P).

Reprint anthology of selected research articles by black mathematicians and mathematics educators, together with a biographical index of black mathematicians. Appendices include data on black mathematicians together with articles and letters concerning the history of discrimination against blacks in the field of mathematics.

Kolata, Gina Bari, *Testing primes gets easier*, Science 209 (26 September 1980) 1503.

A new algorithm for testing whether a large number is a prime. The time required for testing n is on the order of

$$(\log n)^{(\log\log\log n)^2}$$

Steen, L.A., *Mathematical games: from counting votes to making votes count: the mathematics of elections*, Scientific American 243:4 (October 1980) 16-26, 210.

Martin Gardner relinquishes his space to Lynn Steen for a timely exposition on the mathematics of elections. The article discusses how a third-party candidate can win, why elections with more than two candidates are more mathematically messy, and other methods of counting votes besides simple majority rule.

Tape, Walter, *Analytic foundations of halo theory*, J. Optical Society of America 70 (October 1980) 1175-1192.

Presents an analytic framework for systematic computation of halos seen around the sun or moon; the halos result from refraction of light in ice crystals in the atmosphere. Computer-generated figures illustrate the article.

Usiskin, Zalman, *What should not be in the algebra and geometry curricula of average college-bound students?*, Mathematics Teacher 73 (September 1980) 413-424.

For the *average* student, recommends deletion of specific topics, based on three criteria of importance: 1) in understanding or coping in society; 2) for future work in mathematics or applied mathematics; 3) in understanding what mathematics is about. What should go? In algebra: traditional phony word problems (replace with real applications), quadratic factoring (use formula instead), complicated manipulation of fractions which requires factoring; in geometry: some proof, and the least important theorems.

Edwards, C.H., Jr., The Historical Development of the Calculus, Springer-Verlag, 1979; xii + 351 pp, $28.

A splendid book that should be in every college library and on every calculus teacher's desk! It emphasizes the genesis and evolution of the fundamental concepts and techniques that form the heart of the calculus course, without getting bogged down in overly technical details. Historically motivated exercises are inserted in the text at appropriate points.

Fournier, Alain and Fussell, Don, *Stochastic modeling in computer graphics*, Computer Graphics, Special SIGGRAPH 80 issue.

Representing irregular terrain is a difficult problem in computer graphics. The solution given here is to use a stochastic process with (for example) two variables to represent a surface, and then display the surface by taking sample paths along it.

Kolata, Gina Bari, *Hua Lo-Keng shapes Chinese math*, Science 210 (24 October 1980) 413-414.

A man with no earned degrees, 70-year old Hua has exerted great influence on modern Chinese mathematics. His recent visit to the U.S. provided the occasion for this interview. A more detailed biography was given by Steven Salaff in Isis 63 (1972) 142-183.

Harvey, H.R. and Williams, B.J., *Aztec arithmetic: positional notation and area calculation*, Science 210 (31 October 1980) 499-505.

Deciphers and analyzes 16th century Aztec land documents, which use positional line-and-dot notation, a symbol for zero, and some still-unknown method to calculate areas of quadrilaterals. The results imply a mathematical development as sophisticated as that of the Mayas.

Averbach, Bonnie and Chein, Orin, Mathematics: Problem Solving Through Recreational Mathematics, Freeman, 1980; vii + 400 pp, $16.50.

A refreshing and lively text designed to give students a feeling for mathematics in a one- or two-semester "math for poets" course. Topics included are problems from logic, algebraic recreations (i.e., word problems), number theory, cryptorithms, graph theory, games of strategy, and solitaire games and puzzles. The goal is to show "that mathematics is not just numbers and manipulation--it's thinking; it's strategy." Teacher's Manual available.

Kolata, Gina Bari, *Math and sex: are girls born with less ability?*, Science 210 (12 December 1980) 1234-35.

Sure to heat up the argument as to whether mathematical ability is sex-related or a product of societal influences. Data from the Johns Hopkins mathematics talent searches supports the contention of C. Benbow and J. Stanley that boys may have a genetic advantage over girls. Follow-up in *Do males have a math gene*, Newsweek (15 December 1980) 73.

NEWS & LETTERS

"The referee corrected the author, I corrected the referee, you corrected me, and now our secretary says we're ALL wrong!"

NEW EDITOR

Many thanks to Lynn Steen and Arthur Seebach, who, during their five-year term as co-editors of this *Magazine* produced a journal eagerly anticipated by its readers. The S^2 team will be a hard act to follow. The new editor's office is established (with the help of the unique S^2 moving company: Seebach's Studebaker). The new team D^2 (Doris Schattschneider and secretary Dianne Chomko), assisted by an enthusiastic board of associate editors (see p. 1) will produce a *Magazine* which maintains much of the tone, style, and format established by S^2.

Well-written manuscripts on topics of wide interest are always welcome; see pp. 44-45 for our editorial policy. The quality of the *Magazine* depends in large part on the careful work of its referees. Persons willing to serve in this capacity should write to the Editor.

ADDITIONAL PROBLEMS SOLVERS

Due to a change in the printing schedule, copy for the Jan. 1981 issue of the PROBLEMS Section was mailed before the Oct. 1, 1980 deadline for readers to send in solutions to Proposals 1089-1092. The following additional solvers are hereby acknowledged: 1089--J.M. Stark; 1090--Lorraine L. Foster, William Myers, J.M. Stark; 1091--Lorraine L. Foster, Mark F. Kruelle, Bob Prielipp, J.M. Stark; 1092--Hans Kappus (Switzerland), Mary S. Krimmel, Mark F. Kruelle, Hubert Ludwig, Harry Sedinger, Robert S. Stacy, Edward T.H. Wang (Canada), Dennis Wildfogel.

Dan Eustice
PROBLEMS Editor

FINITE SIMPLE GROUPS CLASSIFIED

On August 1 of this year, Michael Aschbacher wrote to Daniel Gorenstein that he had finished the few remaining, standard-form problems and, thereby, had completed the classification of the finite simple groups. This work culminated a twenty-year effort by approximately 300 group theorists around the world. The complete proof will run about 5,000 journal pages.

This past year has been an exciting one for those interested in this problem. Last July, 200 group theorists spent four weeks at a conference at Santa Cruz discussing the remaining difficulties in the classification, as well as exploring new avenues for research for finite group theorists. In the fall of 1979, Enrico Bombieri, a Field's Medalist, solved the long-standing problem about simple groups of Ree type--a problem which John Thompson, another Field's Medalist, had worked on for years. At the AMS meeting in January, 1980, at San Antonio, Michael Aschbacher received the Cole Prize in algebra for his work on the classification. A week later, Robert Griess, Jr., announced that he had constructed the twenty-fifth, sporadic simple group F_1--the Monster. This group consists of 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000 matrices each of size 196,883 × 196,883. A few weeks later, word came from Cambridge that Conway, Norton, Thackrary, and Benson had constructed the twenty-sixth and last, sporadic simple group J_4.

What lies ahead for finite group theorists? Daniel Gorenstein and some others plan to spend much of their time revising the proof. Their goal is to ensure its accuracy, shorten it, and make it more accessible to nonspecialists. George Glauberman once quipped that one of his goals was to reduce the 255-page proof of the Feit-Thompson Theorem to 10 pages and publish it in the *Reader's Digest*. Perhaps the *Reader's Digest* will publish a special issue with the revised version of the classification!

References

[1] Michael Aschbacher, "The Finite Simple Groups and Their Classification," Yale University Press, New Haven, 1980.

[2] Jonathon Friendly, "A school of theorists works itself out of a job," *The New York Times*, Sunday, June 22, 1980, p. E11.

[3] Joseph A. Gallian, "The search for finite simple groups," this *Magazine*, 49 (1976) 163-179.

[4] Martin Gardner, "The capture of the monster: a mathematical group with a ridiculous number of elements," *Scientific American*, 242 (1980) 20-32.

[5] Daniel Gorenstein, "The classification of finite simple groups I. Simple groups and local analysis," *Bulletin (New Series)*, AMS, 1 (1979) 43-199.

[6] Lynn Arthur Steen, "A monstrous piece of research," *Science News*, 118 (1980) 204-206.

Joe Gallian
Associate Editor

GLOBAL ORCHARDING

In formulating the "Tree Planting Problem on a Sphere" (this *Magazine*, Sept. 1980, pp. 235-237), Ruberg does not distinguish between two distinct problems; the small difference in their formulation has far-reaching consequences for the solutions.

Problem 1. Find sets of n points in the plane for which the number of lines containing precisely k of the points is maximal.

Problem 2. Find sets of n points in the plane no $k + 1$ of which are collinear, for which the number of lines containing precisely k of the points is maximal.

Ruberg's original formulation is akin to that of Problem 1, while the explanation of his Table 1 clearly refers to Problem 2 (or, rather, its modification to the sphere).

To see this, consider $k = 3$, and denote by s_n the maximal number of lines solving the analogue of Problem 1 for the sphere (understanding any great circle as "line"); by p_n and r_n we denote, following Ruberg, the corresponding solutions of Problem 2 in the plane and on the sphere.

It is known (see [1]) that
(*) $p_n \geqq 1 + [n(n-3)/6]$
for all $n \geqq 3$; using this it is not hard to show--following Ruberg's argument--that
(**) $r_n \geqq p_{n+1} \geqq 1 + [(n+1)(n-2)/6]$.
To solve Problem 1 on the sphere, Ruberg's argument may be used repeatedly. If it is used j times it follows that $s_n \geqq p_{n-2j} + j(n-2j)$; in particular, taking $j = [(n+6)/8]$ leads to (***) $s_n \geqq [3(n-1)^2/16 + a$, where $a = 0$ if $n \equiv 1 \pmod 8$ and $a = 1$ otherwise. For a few small values of n better results are available, namely $p_7 = 6$, $p_{11} = 16$, $p_{16} = 37$, $p_{19} \geqq 52$. From these, it follows that $r_9 = s_9 = 13$, $r_{13} = 27$, $r_{18} = 53$, $r_{21} \geqq 71$, $s_{11} \geqq 20$, $s_{15} \geqq 38$, $s_{17} \geqq 49$, $s_{20} \geqq 69$, $s_{22} \geqq 85$, $s_{24} \geqq 101$, $s_{25} \geqq 109$, $s_{27} \geqq 128$. It may be conjectured that for all other values of n equality holds in the above estimates (*), (**), (***) for p_n, r_n and s_n.

It is of interest to observe how the few exceptional values of p_n and r_n obscured the pattern of relations sufficiently so that the coincidence of r_n

with p_{n+1} was not recognized from Ruberg's Table 1.

Ruberg's conjecture that if $k = 4$ the solution of Problem 2 for the sphere is $\binom{[n/2]}{2}$ can easily be proved (for example, by a "reduction from $n+2$ to n" type argument). The same expression solves Problem 1 as well. In contrast, in the plane the situation for $k \geq 4$ is very different: for Problem 1 there are examples which show that at least $c_k n^2$ lines are possible, where c_k is a constant depending on k only, while the best available estimates for Problem 2 are of the form $d_k n^{(k-1)/(k-2)}$ (see [2] and [3], for additional references).

References

[1] S.A. Burr, B. Grünbaum, N.J.A. Sloane, "The orchard problem," *Geometriae Dedicata* 2 (1974) 397-424.

[2] B. Grünbaum, "Arrangements and spreads," *CBMS Regional Conference Series in Mathematics*, Vol. 10, Amer. Math. Soc., Providence, RI, 1972.

[3] B. Grünbaum, "New views on some old question of combinatorial geometry," *Colloq. Internaz. Teorie Combinatorie*, Roma 1973, Vol. 1, pp. 451-468, 1976.

Branko Grünbaum
University of Washington
Seattle, WA 98195

THINK FIRST . . .

G.A. Heuer has pointed out that in "Inequalities for a Collection" (this *Magazine*, Jan. 1979, pp. 28-31), Example C is incorrect. In fact, there are no functions satisfying its hypotheses since if $f'(0) < 1$ we have $f(x) < x$ near $x = 0$; if also $f(1) > 1$ we must have $f(x) = 1$ somewhere in between.

The error resulted from an error in numerical computation, providing yet another instance of the adage, "Think first, then compute."

R.P. Boas
Northwestern University
Evanston, IL 60201

1980 WILLIAM LOWELL

A-1. Let b and c be fixed real numbers and let the ten points (j, y_j), $j = 1,2,\ldots,10$, lie on the parabola $y = x^2 + bx + c$. For $j = 1,2,\ldots,9$, let I_j be the point of intersection of the tangents to the given parabola at (j, y_j) and $(j + 1, y_{j+1})$. Determine the polynomial function $y = g(x)$ of least degree whose graph passes through all nine points of I_j.

A-2. Let r and s be positive integers. Derive a formula for the number of ordered quadruples (a,b,c,d) of positive integers such that $3^r \cdot 7^s = \mathrm{lcm}[a,b,c] = \mathrm{lcm}[a,b,d] = \mathrm{lcm}[a,c,d] = \mathrm{lcm}[b,c,d]$. The answer should be a function of r and s.

A-3. Evaluate

$$\int_0^{\pi/2} \frac{1}{1 + (\tan x)^{\sqrt{2}}}\, dx .$$

A-4. (a) Prove that there exist integers a,b,c, not all zero and each of absolute value less than one million, such that $|a + b\sqrt{2} + c\sqrt{3}| < 10^{-11}$.
(b) Let a,b,c be integers, not all zero and each of absolute value less than one million. Prove that

$$|a + b\sqrt{2} + c\sqrt{3}| > 10^{-21}.$$

A-5. Let $P(t)$ be a nonconstant polynomial with real coefficients. Prove that the system of simultaneous equations

$$0 = \int_0^x P(t) \sin t \, dt$$

$$0 = \int_0^x P(t) \cos t \, dt$$

has only finitely many real solutions x.

A-6. Let C be the class of all real valued continuously differentiable functions f on the interval $0 \leq x \leq 1$ with $f(0) = 0$ and $f(1) = 1$. Determine the largest real number u such that

$$u \leq \int_0^1 |f'(x) - f(x)| \, dx$$

for all f in C.

PUTNAM EXAMINATION

B-1. For which real numbers c is
$$(e^x + e^{-x})/2 \leq e^{cx^2}$$
for all real x?

B-2. Let S be the solid in three dimensional space consisting of all points (x,y,z) satisfying the following system of six simultaneous conditions:
$$x \geq 0, \quad y \geq 0, \quad z \geq 0,$$
$$x + y + z \leq 11,$$
$$2x + 4y + 3z \leq 36,$$
$$2x + 3z \leq 24.$$
(a) Determine the number v of vertices of S.
(b) Determine the number e of edges of S.
(c) Sketch in the bc-plane the set of points (b,c) such that (2,5,4) is one of the points (x,y,z) at which the linear function $bx + cy + z$ assumes its maximum value on S.

B-3. For which real numbers a does the sequence defined by the initial condition $u_0 = a$ and the recursion $u_{n+1} = 2u_n - n^2$ have $u_n > 0$ for all $n \geq 0$? (Express the answer in the simplest form.)

B-4. Let $A_1, A_2, \ldots, A_{1066}$ be subsets of a finite set X such that $|A_i| > \frac{1}{2}|X|$ for $1 \leq i \leq 1066$. Prove there exist ten elements $x_1, \ldots, x_{10}$ of X such that every A_i contains at least one of $x_1, \ldots, x_{10}$. (Here $|S|$ means the number of elements in the set S.)

B-5. For each $t \geq 0$, let S_t be the set of all nonnegative, increasing, convex, continuous, real valued functions $f(x)$ defined on the closed interval [0,1] for which $f(1) - 2f(2/3) + f(1/3) \geq t[f(2/3)-2f(1/3)+f(0)]$. Develop necessary and sufficient conditions on t for S_t to be closed under multiplication. (This closure means that, if the functions $f(x)$ and $g(x)$ are in S_t, so is their product $f(x)g(x)$. A function $f(x)$ is convex if and only if $f(su + (1-s)v) \leq sf(u) + (1-s)f(v)$ whenever $0 \leq s \leq 1$.)

B-6. An infinite array of rational numbers $G(d,n)$ is defined for integers d and n with $1 \leq d \leq n$ as follows:

$$G(1,n) = 1/n,$$

$$G(d,n) = \frac{d}{n} \sum_{i=d}^{n} G(d-1, i-1) \text{ for } d > 1.$$

For $1 < d \leq p$ and p prime, prove that $G(d,p)$ is expressible as a quotient s/t of integers s and t with t not an integral multiple of p. (For example, $G(3,5) = 7/4$ with the denominator 4 not a multiple of 5.)

PROGRESS ON PRIMES

It is a stubborn problem in number theory to prove that there are infinitely many primes of the form $n^2 + 1$. Now there is evidence of a different sort to support the conjecture. For each prime number p there appears to be a smallest integer, call it k, for which $4p^2k^2 + 1$ is a prime. This has been checked on the HP9830 for all primes $p \leq 5000$. The largest value of k was only 45; moreover, 84% of the values of k were less than or equal to 10!

References

[1] Daniel Shanks, "A sieve method for factoring numbers of the form $n^2 + 1$," *MTAC* 13 (1959).

[2] M.C. Wunderlich, "On the Gaussian primes on the line $Im(X) = 1$," *Math. of Computation* 27 (1973) pp. 399-400.

Gloria Gagola
Texas A & M University
College Station, TX 77843

ART AND MATH FILMS

Four 16mm color films on art and mathematics, produced by Michele Emmer are available for purchase. Titles are "Symmetry", "Platonic Solids", "Soap Bubbles", and "The Moebius Band". Write to FILM 7, Via Flaminia Km. 11,500, 00118 Roma, Italy.

Editorial Policy

Mathematics Magazine is a journal of collegiate mathematics designed to enrich undergraduate study of the mathematical sciences. Articles in the *Magazine* are intended to be used to supplement undergraduate courses or as the basis for interesting classroom excursions by instructors looking for a new example, a neat proof, or a recent example.

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 a 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 make it realistic for teachers to use them to supplement their regular courses. Short notes appearing in the *Magazine* should be like finely polished classroom handouts; longer articles should be like the text of an inviting undergraduate colloquium lecture. Student projects and interesting studies by math clubs should be possible using articles and notes published in the *Magazine*.

The editor especially invites papers that provide insight into applications of mathematics, that explore the interface between mathematics and computer science, and that probe into interesting but little-known corners in the history of mathematics. We welcome as well other types of contributions: notes on mathematical games, anecdotes, quotations, or cartoons appropriate for end-of-article fillers, cover illustrations, and mathematics-related humor.

Writing and Revising

Unlike a research journal, *Mathematics Magazine* is responsible first to its readers, then to its authors. This means that the suitability of a manuscript for publication depends as much upon the quality of its exposition as on the significance of its content.

Our advice to potential authors is simple: say something new in an appealing way or say something old in a refreshing way. But say it intelligibly, presuming a minimum of technical vocabulary.

Good writing should be vigorous and informal, written in the active voice, and stocked with appropriate examples. Eschew computation; stress instead insight and motivation. Write as if you were talking to a good student while on a long walk. But then illustrate your ideas with appropriate and appealing graphics drawings, tables, diagrams, photographs. Good illustrations not only help convey appropriate intuition but they enhance the appeal of an article and provide a visual relief on the printed page.

The opening sentences or paragraphs of an article are the most important. These should provide an inviting introduction to the entire article, setting it in a context that will make its importance clear and indicating in general terms what is going to be done in the rest of the article. The reader's natural question, "Why should I want to read this?" should be answered in the first few sentences.

Work hard to develop effective transitions between the different parts of your article. A carefully chosen connective word or a suggestive, albeit imprecise, phrase can make the difference between losing your reader's interest or continuing to nurture his environment.

Choose the title with care. Make it short and direct, descriptive of the article's contents.

Our referees have been instructed not only to check mathematical accuracy, but also to give rather detailed suggestions on stylistic matters. The majority of papers are accepted only after some redrafting by the authors, followed by a thorough editing in our office.

Be generous in providing references for related reading since one of our objectives is to encourage readers to pursue ideas further. Bibliographies may well contain suggested reading as well as just the sources actually used.

There are some excellent guides to mathematical exposition available. Read Harley Flanders, "Manual for Monthly Authors", *Amer. Math. Monthly*, 78 (1971) 1-10. Helpful suggestions can also be found in "How to Write Mathematics", 1973, by N.E. Steenrod, P.R. Halmos, M.M. Schiffer, and J.A. Dieudonné, and "Mathematics Into Type", second edition, by Ellen Swanson, both available from the American Mathematical Society.

Format of Manuscripts: ARTICLES and NOTES

Manuscripts should be prepared in a style consistent with the current format of *Mathematics Magazine*. NOTES (generally manuscripts shorter than about 2000 words) should not be sectioned into smaller pieces; the normal connectives of English prose should be sufficient to maintain the logical flow of ideas in an exposition of that length. ARTICLES (generally, longer survey papers) can be sectioned with a few carefully chosen subtitles typed on lines above the paragraph they introduce.

Manuscripts should be typewritten, double-spaced with one-inch margins, with the title, author, and author's address at the top of the first page. Words being defined should be underscored in a black wavy line since it is the policy of *Mathematics Magazine* to boldface words being defined. References should be listed in alphabetical order and numbered consecutively at the end of the article. Format for all bibliographical entries begins as follows: Author (first name or initials, followed by last name), title of article or book (no underlines, quotation marks, or initials). For journal articles, only the first word of the article is capitalized; journal title should be given in the abbreviated form found in *Mathematical Reviews*. Other information should be listed as shown in the following illustration:

Journal.

[2] J. L. Paul, On the sum of the kth powers of the first n integers, Amer. Math. Monthly, 78 (1971) 271-272.

Book titles should be listed with the first letter of every important word capitalized; other information should be listed as shown below:

Book. [18] H. W. Turnbull, editor, The Correspondence of Isaac Newton, Cambridge Univ. Press, 1959-1960, vol. 1, pp. 13-16, and vol. 2, pp. 99-100.

Illustrations should not be interspersed with the text but 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 each illustration in the appropriate locations.) Whether drawing by hand or computer, do not use ball-point pen for illustrations. Fine point nylon tip pens, or artists' drawing pens are best for clear and accurate reproduction. Each illustration should be numbered and referred to by number in the text.

Authors should submit the original manuscript and one copy, and keep one copy as protection against possible loss. Manuscripts and other editorial correspondence should be sent to: *Doris Schattschneider, Editor*
Mathematics Magazine
Moravian College
Bethlehem, PA 18018.

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, N.W.
Washington, DC 20036

MATHEMATICS MAGAZINE VOL. 54, NO. 1, JANUARY 1981