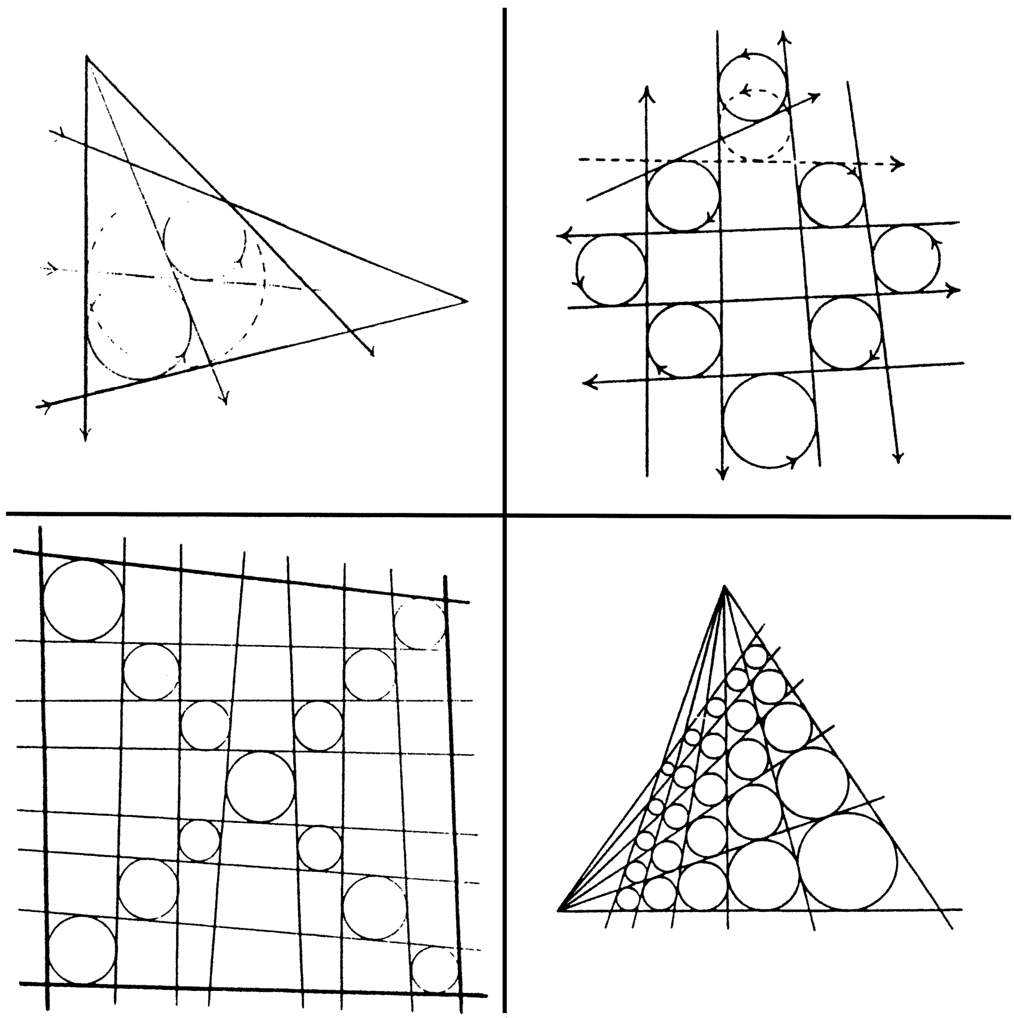
Vol. 64 No. 3, June 1991

MATHEMATICS MAGAZINE



- Cycles and Tangent Rays
- A Nonlinear Recurrence Yielding Binary Digits
- Cubics with a Rational Root

An Official Publication of The MATHEMATICAL ASSOCIATION OF AMERICA

EDITORIAL POLICY

The aim of *Mathematics Magazine* is to provide lively and appealing mathematical exposition. This is not a research journal and, in general, the terse style appropriate for such a journal (lemma-theorem-proof-corollary) is not appropriate for an article for the *Magazine*. Articles should include examples, applications, historical background, and illustrations, where appropriate. They should be attractive and accessible to undergraduates and would, ideally, be helpful in supplementing undergraduate courses or in stimulating student investigations. Articles on pedagogy alone, unaccompanied by interesting mathematics, are not suitable. Neither are articles consisting mainly of computer programs unless these are essential to the presentation of some good mathematics. Manuscripts on history are especially welcome, as are those showing relationships between various branches of mathematics and between mathematics and other disciplines.

The full statement of editorial policy appears in this *Magazine*, Vol. 64, pp. 71–72, and is available from the Editor. Manuscripts to be submitted should not be concurrently submitted to, accepted for publication by, nor published by another journal or publisher.

Send new manuscripts to: Martha Siegel, Editor, Mathematics Magazine, Towson State University, Towson, MD 21204. Manuscripts should be typewritten and double spaced and prepared in a style consistent with the format of *Mathematics Magazine*. Authors should submit the original and two copies and keep one copy. In addition, authors should supply the full five-symbol Mathematics Subject Classification number, as described in *Mathematical Reviews*, 1980 and later. Illustrations should be carefully prepared on separate sheets in black ink, the original without lettering and two copies with lettering added. Do not use staples.

AUTHOR

John F. Rigby received his B.A. and a Ph.D. in group theory from Cambridge University. He was influenced by the books of H. S. M. Coxeter, and reconverted to geometry. Now a Reader in Pure Mathematics at the University of Wales College of Cardiff, he is a great believer in the value of visual insight in the study of geometry. He is currently working on hyperbolic tessellations and triangle geometry. The present article developed from a desire to unify and simplify several results on circles and tangents that have appeared in *Mathematics Magazine* in recent years.

Vol. 64 No. 3, June 1991

MATHEMATICS MAGAZINE

The *MATHEMATICS MAGAZINE* (ISSN 0025–570X) is published by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, D.C. 20036 and Montpelier, VT, bimonthly except July/August.
The annual subscription price for the MATHEMATICS MAGAZINE to an individual member of the Association is $16 included as part of the annual dues. (Annual dues for regular members, exclusive of annual subscription prices for MAA journals, are $64. Student and unemployed members receive a 66% dues discount; emeritus members receive a 50% discount; and new members receive a 40% dues discount for the first two years of membership.) The nonmember/library subscription price is $68 per year.
Subscription correspondence and notice of change of address should be sent to the Membership/Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036. Microfilmed issues may be obtained from University Microfilms International, Serials Bid Coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

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

Postmaster: Send address changes to Mathematics Magazine Membership/Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036-1385.

PRINTED IN THE UNITED STATES OF AMERICA

ARTICLES

Cycles and Tangent Rays

J. F. RIGBY
University of Wales College of Cardiff
Cardiff CF2 4AG, Wales

1. Introduction: Circles Touching Quadrilaterals

Recent articles [2] and [3] in *Mathematics Magazine* are concerned with *circumscribing quadrilaterals*, i.e., sets of four lines touching a circle. The quadrilaterals in these articles are assumed to be convex, and some of the results may be stated briefly as follows. Given the various situations illustrated in FIGURES 1–4, the four heavy lines in each figure touch a circle (these figures are intended to show, without the need of verbal description, various situations of lines touching circles; the arrows in FIGURES 1, 3, and 15 will be explained later). The situation in FIGURE 4 can be extended to a similar situation with n^2 circles: In FIGURE 5 the heavy lines touch a circle. Various other interesting results appear during the proofs of these properties. For instance, in FIGURE 6, $AB + CD = BC + DA$; in FIGURE 7, $AB = CD = EF$; in FIGURE 3, $AC = BD$.

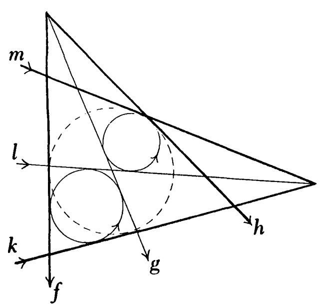


FIGURE 1

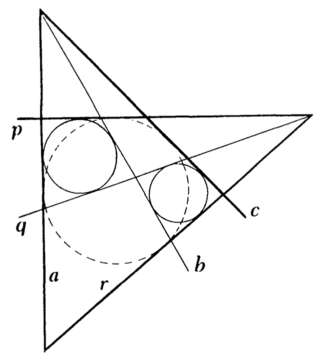


FIGURE 2

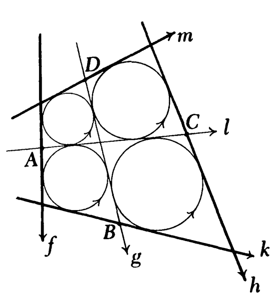


FIGURE 3

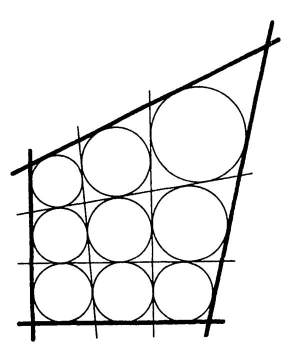


FIGURE 4

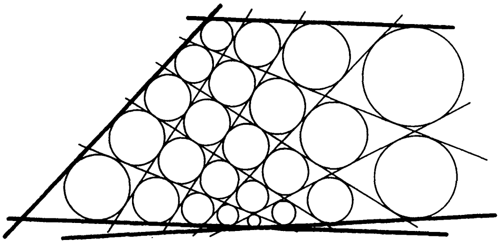


FIGURE 5

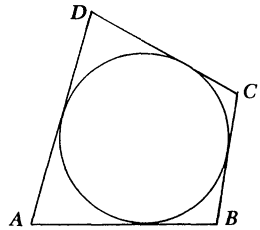


FIGURE 6

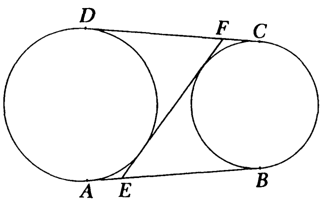


FIGURE 7

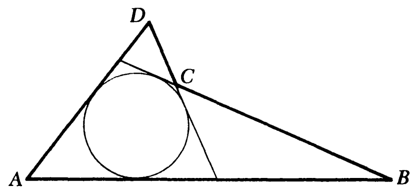


FIGURE 8

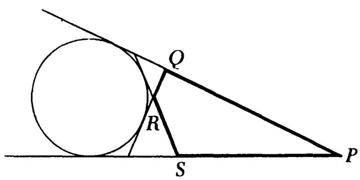


FIGURE 9

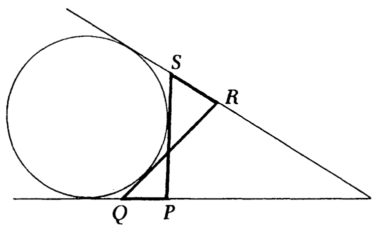


FIGURE 10

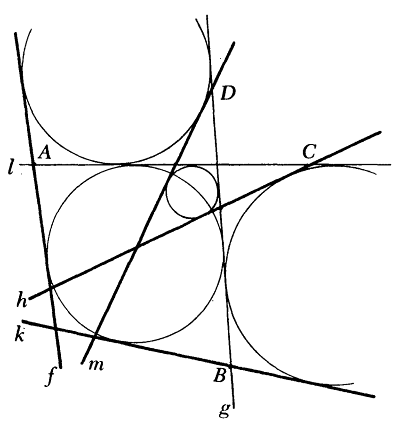


FIGURE 11

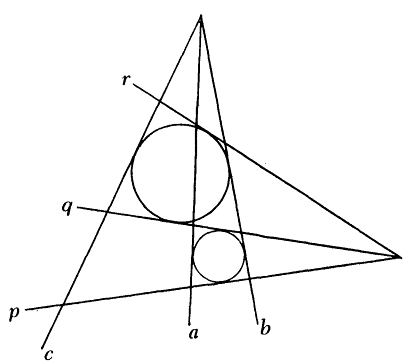


FIGURE 12

Now the result in FIGURE 6 is also true for the non-convex quadrilateral in FIGURE 8: $AB + CD = BC + DA$; whereas in FIGURES 9 and 10 we have $PQ - RS = SP - QR$. Also the results in FIGURE 3 remain true in FIGURE 11: The heavy lines touch a circle and $AC = BD$. On the other hand, FIGURE 12 seems to have the same properties as FIGURE 2: a, b, p, q touch a circle and b, c, q, r touch a circle; but a, c, p, r do *not* touch a circle in FIGURE 12.

So, how can we state the various results and amend the proofs so that they remain valid in more general situations, and how can we explain why things go wrong in FIGURE 12 for instance?

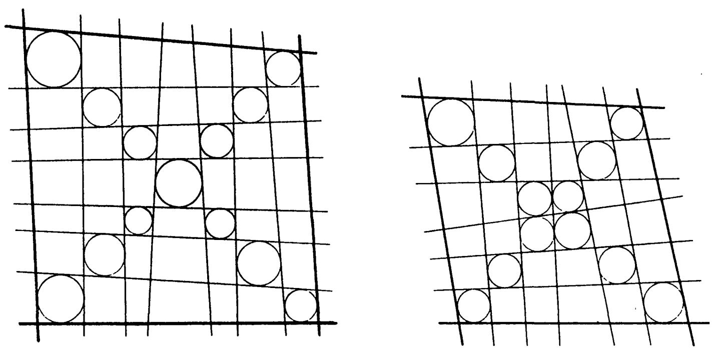


FIGURE 13

In the course of answering these questions we shall find interesting generalizations with very little extra effort: The results of FIGURE 1, 2, and 3 are all special cases of a single, more general theorem, and the conclusion in FIGURE 5 that the four heavy lines touch a circle remains true in the much more general situations shown in FIGURE 13. It is shown in [3] that, whenever there exist n^2 circles as illustrated in FIGURES 4 and 5, the four heavy lines touch a circle; but when do the n^2 circles exist? Examples of this situation are given in [2] and [4] only when the lines are concurrent in two points as in FIGURE 14, but we shall show in the present paper that a figure of n^2 circles like FIGURE 4 or 5 can occur in more general circumstances, as a consequence of the following result: In FIGURE 15 the four heavy lines touch a circle. This result is itself a special case of the theorem illustrated in FIGURE 16 where the four heavy lines touch a circle.

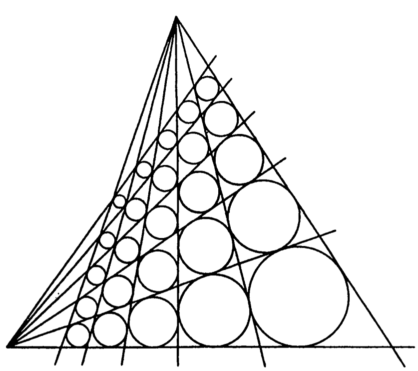


FIGURE 14

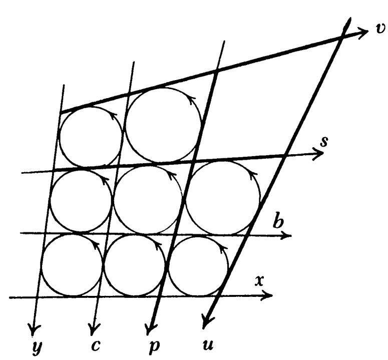


FIGURE 15

2. Cycles and Rays

As a first step we must start thinking in terms of cycles and rays rather than circles and lines. A *cycle* is a circle with a "direction", "sense", or "orientation" assigned to it and indicated in figures by an arrow. This is an intuitive definition but it is sufficient for our present purpose and is more helpful than a formal definition. A *ray* is a line with a direction assigned to it. Two cycles, or a cycle and a ray, *touch* each other or are *tangent* to each other if their directions at the point of touching are the same. Thus in FIGURE 17 the cycles α and β touch each other, as do the cycle α and the ray r; on the other hand β and r *anti-touch* each other.

If r is a ray, the ray along the same line but with opposite direction is the ray *opposite* to r, denoted by $\bar{r}$. We define *opposite cycles* similarly. In most of our results we shall be concerned with cycles and rays that touch rather than anti-touch.

If A and B are points on a ray r, the length AB *relative to* r, denoted by AB_r, is defined to be positive if A comes before B as we travel in the direction of r, and is negative if A comes after B. Thus in FIGURE 17 AB_r is positive, but BA_r is negative and $BA_r = -AB_r$. Also $AB_{\bar{r}} = -AB_r$. For *all* positions of A, B, and C on the ray r we have

$$AB_r + BC_r = AC_r.$$

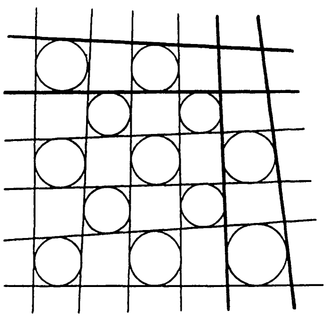


FIGURE 16

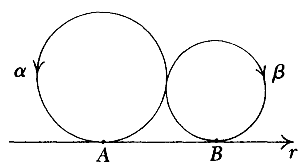


FIGURE 17

If we are dealing with a definite ray and not with its opposite, we can write AB rather than AB_r.

In a situation such as that shown in FIGURE 18, where cycles α and β touch r at R and X, we shall denote the length RX_r by $\alpha\beta_r$. If cycles α, β, γ all touch r, then

$$\alpha\beta_r + \beta\gamma_r = \alpha\gamma_r.$$

In FIGURE 19 we shall denote RS_r by αS_r.

If the rays p, q, r, s touch a cycle we shall write $(pqrs)$; if they touch the cycle α we shall write $(pqrs)_\alpha$. Also if p, q, r touch α we shall write $(pqr)_\alpha$. The notation $(pqrs)$ does not imply that p, q, r, s touch a cycle *in that particular cyclic order*. For instance, in FIGURES 20(a) and (b) we have $(pqrs)$, and both figures illustrate Theorem 3.3, but the cyclic order of the rays in FIGURE 20(b) is p, r, q, s. Thus many of the figures in this article illustrate only one aspect of a theorem, with rays touching cycles in a particular cyclic order.

Two rays are *parallel* if their lines are parallel and their directions are the same; two rays are *anti-parallel* if their lines are parallel but their directions are opposite.

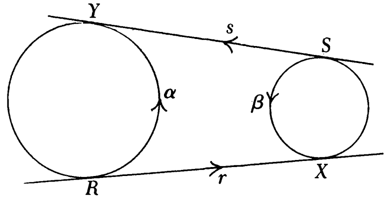


FIGURE 18

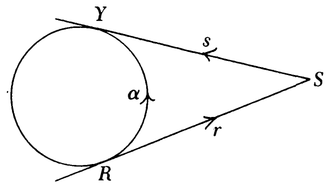
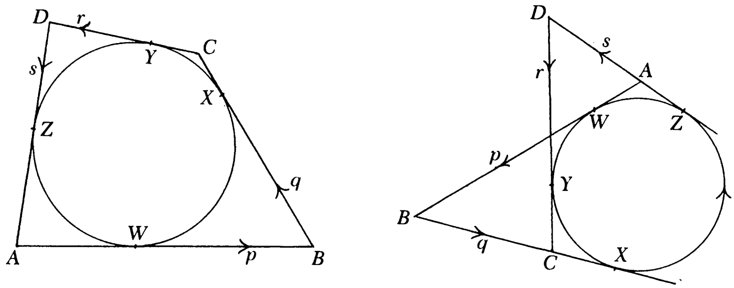


FIGURE 19



(a) FIGURE 20 (b)

3. Basic Results

All our proofs are based on the following basic property.

LEMMA 3.1. *In* FIGURE 18, $\alpha\beta_r = \beta\alpha_s$.

The order of the letters in Lemma 3.1 is important; the lemma states that $RX = SY$, and *not* that $RX = YS$. As a special case, when the cycle β "shrinks to a point" we have

LEMMA 3.2. *In* FIGURE 19, $\alpha S_r = S\alpha_s$ *(or,* $RS = SY$*).*

THEOREM 3.3 (FIGURE 20). *If the quadrilateral ABCD (this is a quadrilateral of rays rather than lines) touches a cycle, then* $AB - BC + CD - DA = 0$.

Proof. Let the rays touch the cycle at W, X, Y, Z as shown. Then $AB - BC + CD - DA = AW + WB - BX - XC + CY + YD - DZ - ZA = 0$ by Lemma 3.2.

The condition in Theorem 3.3 is often given as a necessary and sufficient condition for a quadrilateral to touch a cycle, but there are two difficulties. (i) How do we formulate Theorem 3.3 or its converse in FIGURE 21 where two adjacent rays of the quadrilateral are anti-parallel? (ii) The converse of Theorem 3.3 is not true in FIGURE 22: $CD = -AB$ and $DA = -BC$, so that $AB - BC + CD - DA = 0$, but the four rays do not touch a cycle!

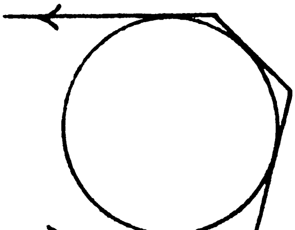


FIGURE 21

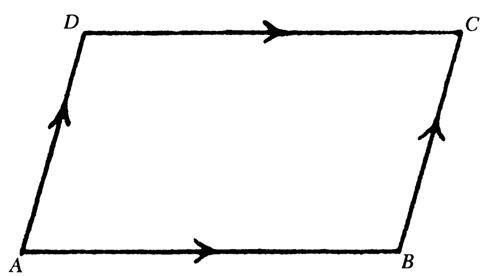


FIGURE 22

Instead of Theorem 3.3 and its converse we shall use Theorem 3.4, which appears at first sight more complicated but which surmounts both the difficulties. Here the vertices A, B, C, D of Theorem 3.3 (FIGURE 20) are replaced by cycles α, β, γ, δ (FIGURES 23, 24, 25) that can be thought of as "generalized vertices."

THEOREM 3.4 (FIGURES 23, 24, 25). *Let p, q, r, s be distinct rays, and α, β, γ, δ cycles, with p touching α and β, q touching β and γ, r touching γ and δ, s touching δ and α.*

(a) *If $(pqrs)$, or if $p \parallel r$ and $q \parallel s$, then $\alpha\beta_p - \beta\gamma_q + \gamma\delta_r - \delta\alpha_s = 0$.*

(b) *Conversely, if p, q, r, s are distinct and if*

$$\alpha\beta_p - \beta\gamma_q + \gamma\delta_r - \delta\alpha_s = 0,$$

then either $(pqrs)$ or $p \parallel r$ and $q \parallel s$.

Proof. (a) If $(pqrs)_\theta$ as in FIGURE 23 then

$$\alpha\beta_p - \beta\gamma_q + \gamma\delta_r - \delta\alpha_s = \alpha\theta_p + \theta\beta_p - \beta\theta_q - \theta\gamma_q + \gamma\theta_r + \theta\delta_r - \delta\theta_s - \theta\alpha_s$$
$$= 0 \quad \text{(using 3.1 four times)}.$$

If $p \parallel r$, $q \parallel s$ as in FIGURE 24, then

$$\begin{aligned}
&\alpha\beta_p - \beta\gamma_q + \gamma\delta_r - \delta\alpha_s \\
&= \alpha A_p + AB_p + B\beta_p - \beta B_q - BC_q - C\gamma_q \\
&\quad + \gamma C_r + CD_r + D\delta_r - \delta D_s - DA_s - A\alpha_s \\
&= (AB_p + CD_r) - (BC_q + DA_s) \quad \text{(using 3.1 four times)} \\
&= 0.
\end{aligned}$$

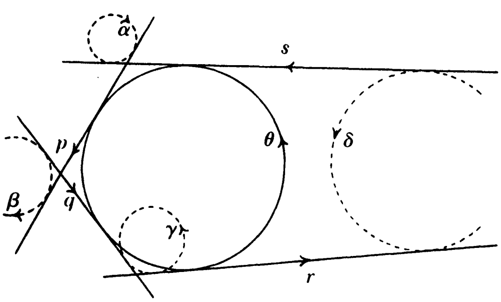


FIGURE 23

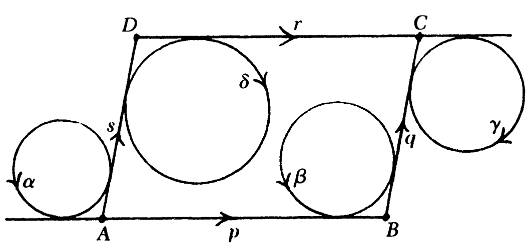


FIGURE 24

If p and r are parallel, and if q and s are anti-parallel to them, as in FIGURE 25, the reader will easily prove that

$$\alpha\beta_p - \beta\gamma_q + \gamma\delta_r - \delta\alpha_s = 0.$$

(b) Suppose conversely that $\alpha\beta_p - \beta\gamma_q + \gamma\delta_r - \delta\alpha_s = 0$ with p, q, r, s distinct. We note that p can be parallel only to r, and q only to s, so either $p \parallel r$ and $q \parallel s$ or, without loss of generality, p is not parallel to r.

In this second case there exist a cycle θ touching p, q, r and a cycle ϕ touching p, r, s (FIGURE 26). Then

$$\begin{aligned} 0 = \alpha\beta_p - \beta\gamma_q + \gamma\delta_r - \delta\alpha_s &= \alpha\phi_p + \phi\theta_p + \theta\beta_p - \beta\theta_q - \theta\gamma_q \\ &\quad + \gamma\theta_r + \theta\phi_r + \phi\delta_r - \delta\phi_s - \phi\alpha_s \\ = \phi\theta_p + \theta\phi_r. \end{aligned}$$

Now $\phi\theta_p = \theta\phi_r$ by Lemma 3.1, so $\theta\phi_r = -\theta\phi_r$. Since p and r are distinct, this implies that $\theta = \phi$ from which the result follows.

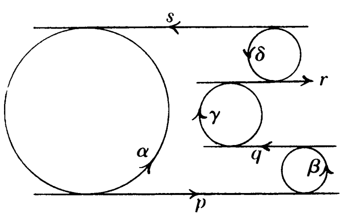


FIGURE 25

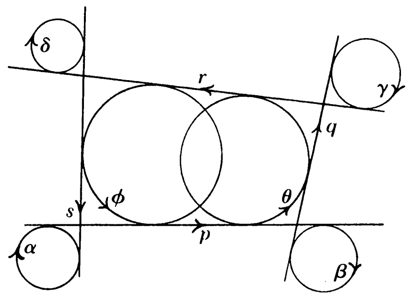


FIGURE 26

4. The Dual of Miquel's Theorem, and a Theorem about Eight Cycles and Rays

The proof of Theorem 4.1 is very easy using Theorem 3.4; the name of the theorem will be explained after the proof.

THEOREM 4.1 (The dual of Miquel's Theorem.) [1, p. 363] (FIGURE 27). *If* $(pqrs)$, $(spzw)_\alpha$, $(pqwx)_\beta$, $(qrxy)_\gamma$, $(rsyz)_\delta$, *then either* $(wxyz)$ *or* $w \parallel y$ *and* $x \parallel z$.

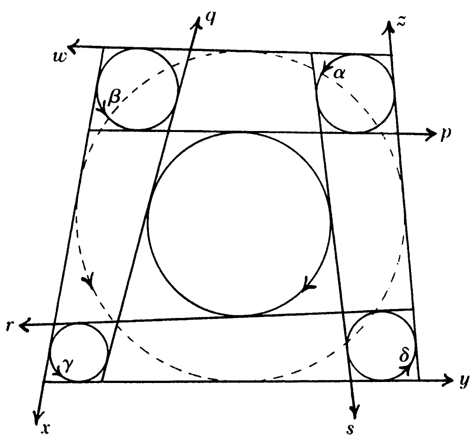


FIGURE 27

Proof. By Theorem 3.4(a), $\alpha\beta_p - \beta\gamma_q + \gamma\delta_r - \delta\alpha_s = 0$; but $\alpha\beta_p = -\alpha\beta_w$ etc., hence

$$-(\alpha\beta_w - \beta\gamma_x + \gamma\delta_y - \delta\alpha_z) = 0.$$

The result now follows by Theorem 3.4(b).

By starting with w, x, y, and z, it is easy to draw a figure to show that the case $w \parallel y$, $x \parallel z$ can actually occur (FIGURE 28).

Miquel's Theorem [1, p. 86] (FIGURE 29) states that if the quadrangles *PQRS*, *PQWX*, *QRXY*, *RSYZ*, *SPZW* are cyclic, then *WXYZ* is cyclic. The only difference between this theorem and Theorem 4.1 is that here we have cyclic quadrangles of points and in Theorem 4.1 we have cyclic quadrilaterals of rays. Coolidge pointed out this duality between point-circle theorems and ray-cycle theorems in Chapter X of [1] where other examples are given also, but there is no general principle of duality such as exists in projective geometry. See Section 6 for a further discussion of this topic.

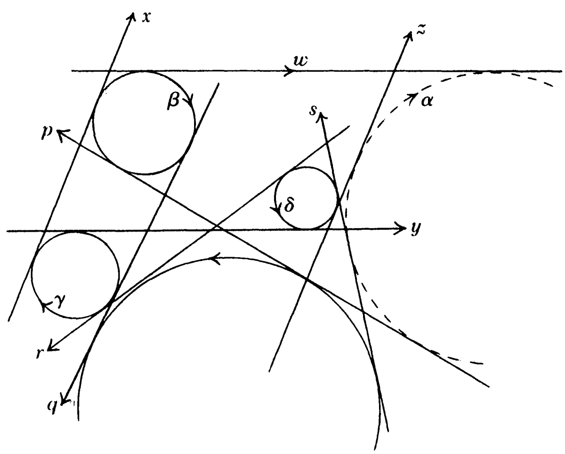


FIGURE 28

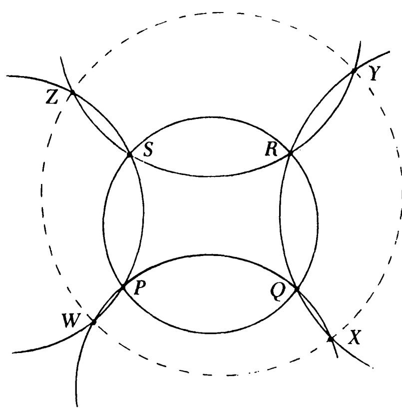


FIGURE 29

FIGURE 29 illustrates the *Miquel Configuration* of circles and points; it is referred to as a $(6_4 8_3)$ configuration because there are six circles each passing through four of the points and eight points each lying on three of the circles. Similarly FIGURE 27 illustrates a $(6_4 8_3)$ configuration of cycles and rays, the dual of the Miquel configuration.

For a different treatment of Miquel's Theorem and its dual, the reader is referred to [5, §§ 94.1, 94.2] where the name "the Six-circles Theorem" is used.

In the special case when $w \parallel y$ and $x \parallel z$, Theorem 4.1 has a converse:

THEOREM 4.2 (FIGURE 28). *If* $(pqrs)$, $(pqwx)_\beta$, $(qrxy)_\gamma$, $(rsyz)_\delta$ *and* $w \parallel y$, $x \parallel z$, *then* $(spzw)_{\alpha'}$.

Proof. The rays p and w are not parallel since they touch β, and similarly p and s are not parallel; also s and y are not parallel, and $y \parallel w$, so s and w are not parallel. Hence there exists a cycle α' touching p, s, w. Let z' be the second common tangent of δ and α'. From the dual of Miquel's Theorem we deduce that $x \parallel z'$ since $w \parallel y$. Hence $z' \parallel z$, so $z' = z$ since both touch δ. Hence $(spzw)_{\alpha'}$.

If we consider the special case of Theorem 4.1 in which $r = \bar{p}$ (the ray opposite to p) and $s = \bar{q}$, then p, q, r, s automatically touch a point-cycle, and so we obtain Theorem 4.3 below after changing the notation.

THEOREM 4.3 (FIGURE 3). *If* $(f\bar{g}k\bar{l})$, $(f\bar{g}l\bar{m})$, $(g\bar{h}k\bar{l})$, $(g\bar{h}l\bar{m})$, *then either* $(f\bar{h}k\bar{m})$ *or* $k \parallel \bar{m}$ *and* $\bar{h} \parallel f$.

Proof. In FIGURE 27, let s coincide with $\bar{q}$, and r with $\bar{p}$, so that the cycle in the centre of the figure becomes a point-cycle. More precisely, we apply Theorem 4.1 with p, q, r, s equal to l, $\bar{g}$, $\bar{l}$, g and w, x, y, z equal to $\bar{m}$, f, k, $\bar{h}$.

THEOREM 4.4 (FIGURE 1). *If the rays* f, g, h, *and also* k, l, m, *are concurrent, and if* $(f\bar{g}k\bar{l})$ *and* $(g\bar{h}l\bar{m})$, *then either* $(f\bar{h}k\bar{m})$ *or* $f \parallel \bar{m}$ *and* $k \parallel \bar{h}$.

Proof. Apply Theorem 4.1 with p, q, r, s equal to $\bar{g}$, $\bar{l}$, l, g and w, x, y, z equal to f, k, $\bar{m}$, $\bar{h}$. (The rays p, q, r, s now touch a point-cycle, and so do q, r, x, y and s, p, z, w.)

By repeated application of Theorem 4.1 (starting if necessary with the special case of Theorem 4.3) we deduce the next result, stated here for convenience in terms of lines and circles rather than rays and cycles.

THEOREM 4.5. *In the situations shown in* FIGURE 13 *the four heavy lines touch a circle.*

THEOREM 4.6. *In* FIGURE 30, $\gamma\alpha_a = \delta\beta_b$.

Proof.

$$2\gamma\alpha_a = \gamma\alpha_a + \alpha\gamma_c = \gamma\mu_a + \mu\lambda_a + \lambda\alpha_a + \alpha\phi_c + \phi\theta_c + \theta\gamma_c$$

$$= \mu\lambda_a + (\gamma\mu_a + \theta\gamma_c) + \phi\theta_c + (\alpha\phi_c + \lambda\alpha_a)$$

$$= \lambda\mu_p + (\mu\gamma_q + \gamma\theta_q) + \theta\phi_r + (\phi\alpha_s + \alpha\lambda_s)$$

$$= \lambda\mu_p + \mu\theta_q + \theta\phi_r + \phi\lambda_s.$$

Similarly $2\delta\beta_b$ is equal to the same expression.

By considering the special case where α, β, γ, δ are point-cycles A, B, C, D, we obtain the following result:

COROLLARY OF THEOREM 4.6. *In the situation of* FIGURE 3, *the lengths AC and BD are equal.*

We shall also need a converse of Theorem 4.6:

THEOREM 4.7 (FIGURE 31). *If* $(acs)_\alpha$, $(bdp)_\beta$, $(caq)_\gamma$, $(dbr)_\delta$, *if* $\gamma\alpha_a = \delta\beta_b = \alpha\gamma_c = \beta\delta_d$, *and if* $(abpq)$, $(bcqr)$, $(cdrs)$, *and if d and a are not parallel, then* $(dasp)$.

Proof. Let ϕ denote the cycle touching c, d, r, s. The rays a, p are not parallel since $(abpq)$; p, d are not parallel since they touch β; d, a are not parallel (given). Hence there exists a cycle λ' touching d, a, p. Let s' be the second common tangent of ϕ and λ'. No two of a, c, s' are parallel; let α' touch a, c, s'. Then $\gamma\alpha'_a = \delta\beta_b$ (by Theorem 4.6) $= \gamma\alpha_a$ (given). This implies that $\alpha' = \alpha$; hence $s' = s$ so λ' touches d, a, s, p.

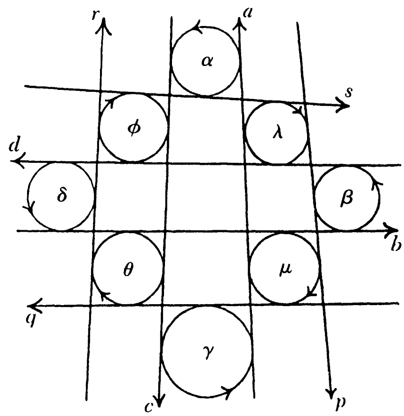


FIGURE 30

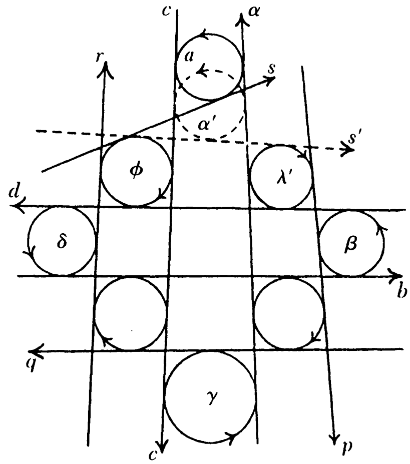


FIGURE 31

5. A Chequer-board Theorem

THEOREM 5.1. *In the situation of* FIGURE 32, *either* $(spzw)$ *or* $z \parallel p$ *and* $w \parallel s$.

Proof. Applying the dual of Miquel's Theorem three times (it will be clear from FIGURE 32 exactly how the theorem is being applied) we have

either $(bazy)$ or $b \parallel z$, $a \parallel y$,
either $(adyx)$ or $a \parallel y$, $d \parallel x$,
either $(dcxw)$ or $d \parallel x$, $c \parallel w$,

from which we deduce that either

(i) $(bazy)$, $(adyx)$ and $(dcxw)$, or
(ii) $b \parallel z$, $a \parallel y$, $d \parallel x$ and $c \parallel w$.

In case (i) we also have $(bdw)_\beta$, $(acz)_\alpha$, $(dby)_\delta$, $(cax)_\gamma$; and $\delta\beta_b = \gamma\alpha_a = \beta\delta_d = \alpha\gamma_c$ by Theorem 4.4. Hence $(cbwz)$ by Theorem 4.7 since c, b are not parallel. (We apply 4.7 with $\alpha\beta\gamma\delta$, $abcd$, $pqrs$ replaced by $\beta\alpha\delta\gamma$, $badc$, $zyxw$). Now in the top right hand portion of FIGURE 32 we have $(cadb)$, $(cazs)$, $(adsp)$, $(dbpw)$, $(bcwz)$, and hence by the dual of Miquel's theorem either $(zspw)$ or $z \parallel p$ and $s \parallel w$.

In case (ii), in the top right hand portion of FIGURE 32 we have $(sadp)$, $(sazc)$, $(adcb)$, $(dpbw)$ and $z \parallel b$, $c \parallel w$. Hence by Theorem 4.2 $(pswz)$. The reader is invited to draw a figure illustrating case (ii).

Considering the special case where $q = \bar{b}$, $d = \bar{s}$, $r = \bar{c}$, $a = \bar{p}$, and writing $\bar{w} = u$, $\bar{z} = v$, we obtain the next result:

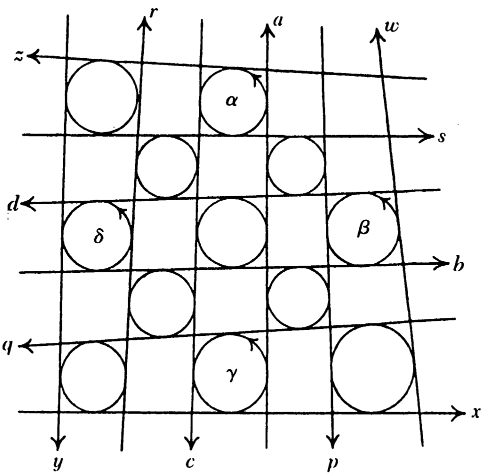


FIGURE 32

THEOREM 5.2 (FIGURE 15). *If* $(x\bar{b}y\bar{c})$, $(x\bar{b}c\bar{p})$, $(x\bar{b}p\bar{u})$, $(b\bar{s}y\bar{c})$, $(b\bar{s}c\bar{p})$, $(b\bar{s}p\bar{u})$, $(s\bar{v}y\bar{c})$, $(s\bar{v}c\bar{p})$, *then either* $(s\bar{v}p\bar{u})$ *or* $\bar{v} \parallel p$ *and* $\bar{u} \parallel s$.

In the bottom left-hand corner of FIGURE 5 we find a figure of the type shown in FIGURE 3. Starting with FIGURE 3 we can now build up FIGURE 5 in a unique way, by repeated application of Theorem 5.2 (FIGURE 15).

6. A Limited Form of Duality

In Section 4 we considered the duality between Theorem 4.1 and Miquel's Theorem. We shall now show that other cycle-ray theorems have circle-point duals, but there is not a complete duality in which every circle-point theorem has a cycle-ray dual and conversely. The ideas in this final section will be presented only briefly.

The starting point of our proofs was Lemma 3.1 concerning *the distance between two cycles along a common tangent ray*. The dual of this concept of distance ought to be *the angle between two circles at a common point*, but it is worth seeing why this dual concept is not strong enough for our purpose.

If two circles α and β meet at R, the angle between α and β at R, denoted by $\alpha\beta_R$, is defined to be the angle between the tangents to the circles at R. This angle is positive or negative according as we turn anticlockwise or clockwise in going from α to β, and is defined only modulo 180°; for instance in FIGURE 33 $\alpha\beta_R = 55°$ or $-125°$. All calculations with angles must be performed modulo 180°. Corresponding to Lemma 3.1 we have the following result: *If two circles* α *and* β *meet at* R *and* S *as in* FIGURE 33, *then* $\alpha\beta_R = \beta\alpha_S$.

Now at the end of the proof of Theorem 3.4 we have two cycles θ and ϕ with two distinct common tangent rays p and r such that $\theta\phi_r = -\theta\phi_r$, and we deduce that $\theta = \phi$. Suppose however that the circles θ and ϕ have two distinct common points P and R such that $\theta\phi_R = -\theta\phi_R$. We cannot deduce that $\theta = \phi$: It is possible to have θ orthogonal to ϕ as in FIGURE 34, since all calculations with angles are performed modulo 180°. Thus we cannot by this method prove a dual of Theorem 3.4 and hence prove Miquel's Theorem. A similar problem arises when we attempt to dualise Theorem 4.6 and its converse 4.7.

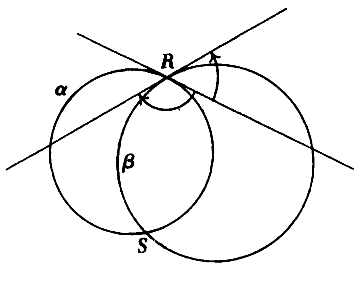


FIGURE 33

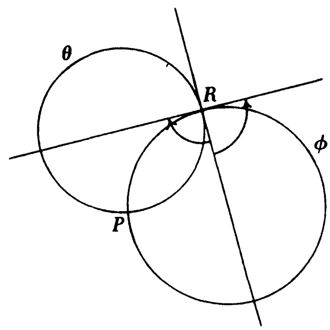


FIGURE 34

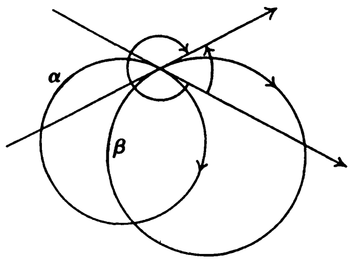


FIGURE 35

We avoid this difficulty in the following surprising way: When attempting to dualise our results about cycles and rays we turn each circle into a cycle by assigning an arbitrary positive direction to it. Then if two cycles α and β meet at R, the angle between α and β at R is defined modulo 360°; for instance in FIGURE 35 $\alpha\beta_R = 55°$ or $-305°$ (we use the same notation as before). All calculations with angles are now performed modulo 360°. Now, if the cycles θ and ϕ have two distinct common points P and R such that $\theta\phi_R = -\theta\phi_R$, we deduce that either $\theta = \phi$ or θ and ϕ are opposite cycles; in either case they are the same circle. We can now dualise the proofs of Theorems 3.4 and 4.1 to provide a proof of Miquel's Theorem. Note that although three rays do not always touch a cycle, three points always lie on a circle (as long as we introduce a single point at infinity and regard lines as circles in the usual way); so the special case of parallel rays has no counterpart for points, and must be ignored when we dualise a theorem.

If we leave Theorem 4.6 in the form $\gamma\alpha_a + \alpha\gamma_c = \delta\beta_b + \beta\delta_d$, with a corresponding change in Theorem 4.7, we find that Theorems 4.6 and 4.7 and their proofs can be dualised; thus the dual of Theorem 5.1 is a theorem. The notion of opposite rays has no counterpart for points, so we cannot expect to dualise theorems in which this notion occurs.

It will now be clear that, subject to the proviso about parallel rays and opposite rays, every theorem about cycles and tangent rays that can be proved using only Theorems 3.4, 4.6 and 4.7 has a dual theorem about circles and points.

Examples do exist of theorems without duals, but we shall not consider them here.

7. Other Approaches

The technique of *Laguerre Inversion*, by means of which certain cycles can be "inverted" into points (see [6] for further references) provided ideas for some of the proofs in this article, but it is more sophisticated than the methods used here and also it does not give complete proofs in all situations.

For a very different treatment of the geometry of cycles and rays (and also the geometry of circles and points) the reader is referred to [7] where the authors start from an abstract axiomatic foundation. I am grateful to Professor Andrew Lenard for drawing my attention to this article.

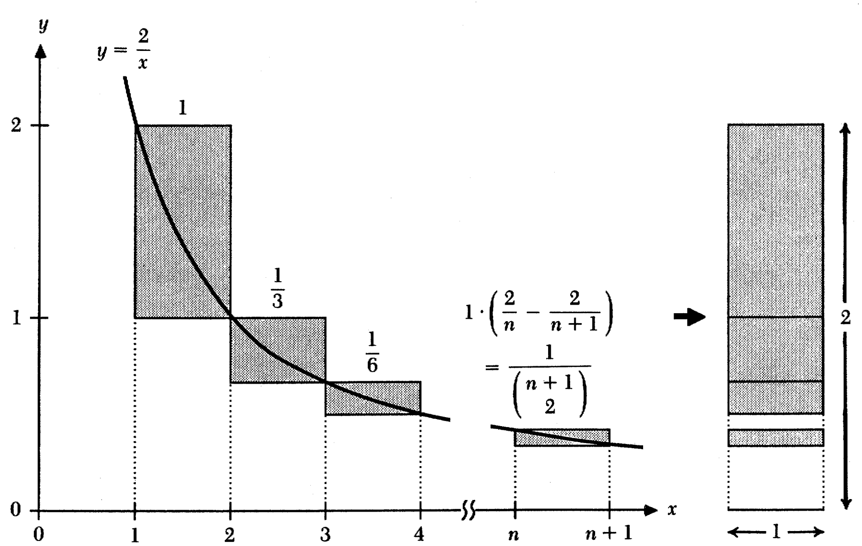
I am grateful to the referees for their helpful comments. FIGURE 14 is adapted from a figure in [3], by kind permission of the author.

REFERENCES

1. J. L. Coolidge, *A Treatise on the Circle and the Sphere*, Oxford 1916.
2. H. Demir and C. Tezer, More on incircles, this MAGAZINE 62 (1989), 107–114.
3. H. Okumura, Configurations arising from the three circle theorem, this MAGAZINE 63 (1990), 116–121.
4. ______, Private communication.
5. D. Pedoe, *A Course of Geometry for Colleges and Universities*, Cambridge University Press, London 1970.
6. J. F. Rigby, The geometry of cycles, and generalized Laguerre inversion, in *The Geometric Vein*, eds. Davis, Grünbaum, Sherk, Springer-Verlag, New York, 1981.
7. B. L. van der Waerden and L. J. Smid, Eine Axiomatik der Kreisgeometrie und der Laguerregeometrie, *Math. Annalen* 110 (1935), 753–776.

Proof without Words:
Sum of reciprocals of triangular numbers

$$\frac{1}{1}+\frac{1}{3}+\frac{1}{6}+\cdots+\frac{1}{\binom{n+1}{2}}+\cdots=2$$



—ROGER B. NELSEN
LEWIS & CLARK COLLEGE
PORTLAND, OR 97219

For a very different treatment of the geometry of cycles and rays (and also the geometry of circles and points) the reader is referred to [7] where the authors start from an abstract axiomatic foundation. I am grateful to Professor Andrew Lenard for drawing my attention to this article.

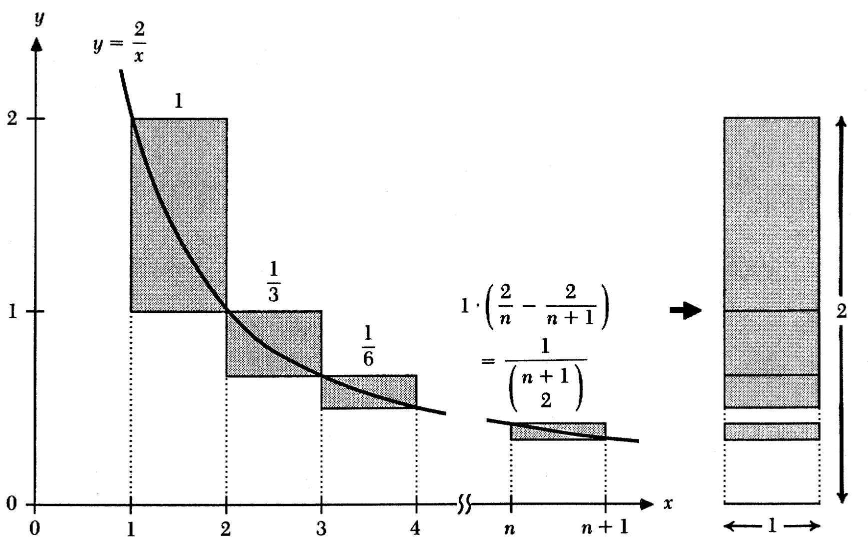
I am grateful to the referees for their helpful comments. FIGURE 14 is adapted from a figure in [3], by kind permission of the author.

REFERENCES

1. J. L. Coolidge, *A Treatise on the Circle and the Sphere*, Oxford 1916.
2. H. Demir and C. Tezer, More on incircles, this MAGAZINE 62 (1989), 107–114.
3. H. Okumura, Configurations arising from the three circle theorem, this MAGAZINE 63 (1990), 116–121.
4. ______, Private communication.
5. D. Pedoe, *A Course of Geometry for Colleges and Universities*, Cambridge University Press, London 1970.
6. J. F. Rigby, The geometry of cycles, and generalized Laguerre inversion, in *The Geometric Vein*, eds. Davis, Grünbaum, Sherk, Springer-Verlag, New York, 1981.
7. B. L. van der Waerden and L. J. Smid, Eine Axiomatik der Kreisgeometrie und der Laguerregeometrie, *Math. Annalen* 110 (1935), 753–776.

Proof without Words:
Sum of reciprocals of triangular numbers

$$\frac{1}{1}+\frac{1}{3}+\frac{1}{6}+\cdots+\frac{1}{\binom{n+1}{2}}+\cdots=2$$



—ROGER B. NELSEN
LEWIS & CLARK COLLEGE
PORTLAND, OR 97219

NOTES

A Nonlinear Recurrence Yielding Binary Digits

STANLEY RABINOWITZ
Westford, MA 01886

PETER GILBERT
Digital Equipment Corporation
Nashua, NH 03060

Graham and Pollak [2] considered the sequence

$$1, 2, 3, 4, 6, 9, 13, 19, 27, 38, 54, 77, \ldots$$

defined by the recurrence

$$u_1 = 1, u_{n+1} = \left\lfloor \sqrt{2}\left(u_n + \tfrac{1}{2}\right)\right\rfloor, \qquad n \geqslant 1,$$

where $\lfloor x \rfloor$ denotes the floor of x, the largest integer not larger than x. They discovered the unusual property that $u_{2n+1} - 2u_{2n-1}$ is just the nth digit in the binary expansion of $\sqrt{2}$. In discussing this result, Erdős and Graham [1] say, "It seems clear that there must be similar results for $\sqrt{m}$ and other algebraic numbers, but we have no idea what they are."

In this paper, we give a generalization of this result and obtain a recurrence relation that yields, in a similar manner, the nth digit in the binary expansion of any positive real number.

We begin by proving some properties of the floor function:

Definition. Let $\{x\}$ denote the fractional part of x, that is, $\{x\} = x - \lfloor x \rfloor$.

Lemma 1. $\lfloor a\lfloor x \rfloor + c \rfloor = \lfloor ax \rfloor$ *if and only if* $\lfloor \{ax\} - a\{x\} + c \rfloor = 0$.

Proof. The following equations are equivalent to each other in succession:

$$\begin{aligned} \lfloor a\lfloor x \rfloor + c \rfloor &= \lfloor ax \rfloor \\ \lfloor ax - a\{x\} + c \rfloor &= \lfloor ax \rfloor \\ \lfloor \{ax\} + \lfloor ax \rfloor - a\{x\} + c \rfloor &= \lfloor ax \rfloor \\ \lfloor \{ax\} - a\{x\} + c \rfloor &= 0. \end{aligned}$$

Lemma 2. *If k is an integer, a is a real number in the range $1 < a < 2$, and $x = k/(a-1)$, then*

$$\left\lfloor a\lfloor x \rfloor + \frac{a}{2} \right\rfloor = \lfloor ax \rfloor.$$

Proof. If $x = k/(a-1)$, then $ax = x + k$ and $\{ax\} = \{x\}$. Thus

$$f(x) = \{ax\} - a\{x\} + \frac{a}{2} = \{x\} - a\{x\} + \frac{a}{2} = \{x\}\left(1 - \frac{a}{2}\right) + (1 - \{x\})\frac{a}{2}.$$

Clearly, $f(x) \geqslant 0$ and $f(x) < 1(1-(a/2)) + 1(a/2) = 1$. Hence $\lfloor f(x) \rfloor = 0$ and the result follows by Lemma 1.

LEMMA 3. *If k is an integer, a is a real number in the range $0 < a < 2$, and $x = k/(2-a)$, then*

$$\left\lfloor a\lfloor x \rfloor + \frac{a}{2} \right\rfloor = \lfloor ax \rfloor.$$

Proof. From $x = k/(2-a)$ we get $2x = ax + k$. Taking the fractional part of both sides yields $\{2x\} = \{ax\}$. It is easy to show that $d = 2\{x\} - \{2x\}$ is always 0 or 1, so we may write $\{2x\}$ as $2\{x\} - d$. Thus

$$f(x) = \{ax\} - a\{x\} + \frac{a}{2} = \{2x\} - \frac{a}{2}(\{2x\} + d) + \frac{a}{2}$$
$$= \{2x\}\left(1 - \frac{a}{2}\right) + \frac{a}{2}(1-d).$$

Clearly $f(x) \geqslant 0$ and $f(x) < 1(1-(a/2)) + (a/2)1 = 1$. Hence $\lfloor f(x) \rfloor = 0$ and the result follows by Lemma 1.

THEOREM. *Given a positive real number w, let $b = (2^{m+1} + w)/(2^m + w)$ and $a = 2/b$, where $m = \lfloor \log_2 w \rfloor$. Define a sequence u_n by the recurrence*

$$u_1 = 1$$
$$u_{n+1} = \begin{cases} \lfloor a(u_n + 1/2) \rfloor, & \text{if } n \text{ is odd} \\ \lfloor b(u_n + 1/2) \rfloor, & \text{if } n \text{ is even}. \end{cases}$$

Then

(i)
$$u_{2n} = \lfloor 2^{n-m-1}(2^m + w) \rfloor$$
$$u_{2n+1} = \lfloor 2^{n-m-1}(2^{m+1} + w) \rfloor.$$

(ii) $u_{2n+1} - 2u_{2n-1}$ *is the nth digit in the binary expansion of w. (The radix point appears after the $(m+1)$st digit.)*

(iii) $u_{2n+2} - 2u_{2n}$ *is the $(n+1)$st digit of the binary expansion of w.*

(iv)
$$u_{2n+1} - u_{2n} = 2^{n-1}.$$

Proof. First note that $1 < b < 2$ and $1 < a < 2$. Also, a little algebra shows that $1 + w/2^m = 1/(b-1)$ and $2 + w/2^m = 2/(2-a)$.

We will prove property (i) by induction on the subscript of u. For $n = 0$, our formula specifies

$$u_1 = \lfloor 2^{-m-1}(2^m + w) \rfloor = \left\lfloor 2^{-1}\left(1 + \frac{w}{2^m}\right) \right\rfloor.$$

But m has been chosen so that $1 \leqslant w/2^m < 2$, which implies that $u_1 = 1$ and our formula checks for $n = 0$. There are now two cases, the subscript being even or odd.

If the result is true for u_{2n}, then we have $u_{2n} = \lfloor x \rfloor$ where

$$x = 2^{n-m-1}(2^m + w) = 2^{n-1}\left(1 + \frac{w}{2^m}\right) = 2^{n-1}\frac{1}{b-1}.$$

Then

$$\begin{aligned} u_{2n+1} &= \left\lfloor bu_{2n} + \frac{b}{2}\right\rfloor = \left\lfloor b\lfloor x \rfloor + \frac{b}{2}\right\rfloor \\ &= \lfloor bx \rfloor \qquad \text{(by Lemma 2)} \\ &= \left\lfloor 2^{n-1}\frac{b}{b-1}\right\rfloor = \lfloor 2^{n-m-1}(2^{m+1} + w)\rfloor \end{aligned}$$

and the result is true for u_{2n+1}.

If the result is true for u_{2n+1}, then we have $u_{2n+1} = \lfloor x \rfloor$ where

$$x = 2^{n-m-1}(2^{m+1} + w) = 2^{n-1}\left(2 + \frac{w}{2^m}\right) = 2^n\frac{1}{2-a}.$$

Then

$$\begin{aligned} u_{2n+2} &= \left\lfloor au_{2n+1} + \frac{a}{2}\right\rfloor = \left\lfloor a\lfloor x \rfloor + \frac{a}{2}\right\rfloor \\ &= \lfloor ax \rfloor \qquad \text{(by Lemma 3)} \\ &= \left\lfloor 2^n\frac{a}{2-a}\right\rfloor = \lfloor 2^{n-m}(2^m + w)\rfloor \end{aligned}$$

and the result is true for u_{2n+2}. This concludes the induction.

Property (ii) is a direct consequence of property (i). The nth binary digit of the number $w = d_1d_2d_3 \cdots d_m d_{m+1}.d_{m+2}d_{m+3}d_{m+4} \cdots$ can be found as follows:

$$2^{n-m-1}w = d_1d_2d_3 \cdots d_n.d_{n+1}d_{n+2}d_{n+3} \cdots$$

and

$$2^{n-m-2}w = d_1d_2d_3 \cdots d_{n-1}.d_nd_{n+1}d_{n+2}d_{n+3} \cdots$$

so

$$\begin{aligned} u_{2n+1} - 2u_{2n-1} &= \lfloor 2^{n-m-1}(2^{m+1} + w)\rfloor - 2\lfloor 2^{n-m-2}(2^{m+1} + w)\rfloor \\ &= \lfloor 2^{n-m-1}w \rfloor - 2\lfloor 2^{n-m-2}w \rfloor \\ &= d_1d_2 \cdots d_n - d_1d_2 \cdots d_{n-1}0 = d_n. \end{aligned}$$

The proof of property (iii) is similar.

Property (iv) follows from the fact that property (i) may be rewritten as

$$\begin{aligned} u_{2n} &= 2^{n-1} + \lfloor 2^{n-m-1}w \rfloor \\ u_{2n+1} &= 2^n + \lfloor 2^{n-m-1}w \rfloor. \end{aligned}$$

We should note that the result of Graham and Pollak follows from our result when $w = \sqrt{2}$. In that case, $m = 0$ and $a = b = \sqrt{2}$. It should also be noted that when we speak of the nth digit of a number, we start counting at the leftmost non-zero digit. If $m < 0$, there will be $|m| - 1$ zeroes after the radix point before the first non-zero binary digit occurs.

To avoid having to consider the even and odd cases separately, our theorem may be rephrased in the following form (by setting $v_n = u_{2n-1}$):

THEOREM (alternate formulation). *Let w be a positive real number and let a and b be defined as before. Define a sequence v_n by the recurrence*

$$v_1 = 1$$
$$v_{n+1} = \left\lfloor b\left\lfloor av_n + \frac{a}{2}\right\rfloor + \frac{b}{2}\right\rfloor.$$

Then $v_{n+1} - 2v_n$ is the nth digit in the binary expansion of w.

If we are only interested in the digits comprising the fractional part of w, we have a slightly simpler result, not involving the variable m. The proof mimics the proof of the main theorem and we leave the details as an exercise for the reader.

THEOREM. *Given a positive real number w, let $b = (2 + w)/(1 + w)$ and $a = 2/b$. Define a sequence u_n by the recurrence*

$$u_1 = \lfloor 2 + w \rfloor$$
$$u_{n+1} = \begin{cases} \lfloor a(u_n + 1/2)\rfloor, & \text{if } n \text{ is odd} \\ \lfloor b(u_n + 1/2)\rfloor, & \text{if } n \text{ is even.} \end{cases}$$

Then $u_{2n+2} - 2u_{2n}$ is the nth digit to the right of the radix point in the binary expansion of w.

The reader may wonder how the authors came up with the values of a, b, and m in the main theorem. We found that if we let $u_{n+1} = \lfloor a(u_n + \frac{1}{2})\rfloor$ and then tried various a's other than $\sqrt{2}$, the quantity $u_{2n+2} - 2u_{2n}$ did not always yield binary digits (0's or 1's). Then we tried changing a to two values, a and b, for the odd and even values of n. Using a computer, we varied a and b and printed out those cases where $u_{2n+2} - 2u_{2n}$ always generated binary digits. We were rewarded by finding that in such cases, $ab = 2$; and when $1 < a < 3/2$, we found that the value of w that was generated appeared to have the value $2(a - 1)/(2 - a)$. This gave us a conjecture on how to get the binary digits for any w between 1 and 2 by picking the values $a = 2(1 + w)/(2 + w)$ and $b = 2/a$. Finally, we realized that if w was not between 1 and 2, we could multiply it by 2^m for some m to bring it into that range and then apply the simpler version of the theorem.

There are other open questions that the reader might wish to pursue. For example, suppose we define u_{n+1} in terms of three quantities, a, b, and c, depending upon whether n is congruent to 0, 1, or 2 (mod 3). For what choices of a, b, and c will $u_{2n+2} - 2u_{2n}$ yield binary digits? Perhaps one should look at $u_{2n+2} - 3u_{2n}$ instead (or maybe $u_{3n+3} - 3u_{3n}$) and try to get digits in base 3.

REFERENCES

1. P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, L'Enseignement Mathématique, Genève, 1980, p. 96.
2. R. L. Graham and H. O. Pollak, Note on a nonlinear recurrence related to $\sqrt{2}$, this MAGAZINE, 43 (1970), 143–145.

Cubics with a Rational Root

WILLIAM C. SCHULZ
Northern Arizona University
Flagstaff, AZ 86011

The equation $y^3 + by^2 + cy + d = 0$ may be transformed into the standard form $x^3 + px + q = 0$ by the transformation $y = x - (b/3)$. The transformed equation was solved by Niccolo Tartaglia in the 16th century [1] by the method described below. If either equation has a rational root, the other will also. However, in contrast to the situation with quadratic equations, the computations carried out in the case of a rational root involve certain irrational, perhaps even complex, quantities. Historically, this represents the first serious involvement European mathematicians had with complex numbers.

From a number theoretic point of view, it is interesting to investigate which irrational quantities appear in the application of Tartaglia's formula to equations with rational p and q and one or more rational roots. Although the process usually involves quantities from two distinct quadratic fields, we shall show exactly which special cases involve one quadratic field or just rational numbers.

Solving the cubic $x^3 + px + q$ by Tartaglia's method we have

$$X = H + K$$

where

$$H = \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} \qquad K = \sqrt[3]{-\frac{q}{2} - \sqrt{\Delta}}$$
$$\Delta = \left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3. \tag{1}$$

In addition, the derivation of these equations requires that $3HK = -p$, which determines the choice of K once H has been chosen. We then have all three roots:

$$x_1 = H + K$$
$$x_2 = \omega H + \omega^2 K \qquad \text{where } \omega = \frac{-1 + i\sqrt{3}}{2}. \tag{2}$$
$$x_3 = \omega^2 H + \omega K.$$

We note that $x_1 + x_2 + x_3 = 0$ since the coefficient of x^2 in the equation is 0.

When the cubic has rational coefficients and a rational root, H and K may still be irrational. We wish to use a bit of the theory of fields to clarify what kind of irrationals are involved. In particular, we will show that if the cubic equation has a rational root, then $-q/2 + \sqrt{\Delta}$ is a perfect cube in the number field $Q[\sqrt{\Delta}\,]$. In what follows we always assume that p and q are rational numbers.

We recall a few definitions and simple theorems from the theory of fields. If α is a root of an irreducible algebraic equation $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ with rational coefficients, then $Q[\alpha]$ is the smallest field containing α and the rationals Q. Its elements have the form

$$\gamma = r_1 \cdot 1 + r_2\alpha + \cdots + r_n\alpha^{n-1} \quad \text{where } r_i \in Q$$

and $Q[\alpha]$ may be regarded as a vector space over Q of dimension n. We call n the relative degree of $Q[\alpha]$ over Q. If we repeat the process using an irreducible algebraic equation of degree m with coefficients from $F = Q[\alpha]$ rather than Q we get an extension $F[\beta]$. Since $\alpha^i\beta^j$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$, is easily seen to be a basis, the dimension of $F[\beta]$ as a vector space over Q is mn. We will use the notation $m = [F[\beta]:F]$ and $n = [F:Q]$ so we may write the last relationship as

$$[F[\beta]:Q] = [F[\beta]:F][F:Q].$$

A similar multiplicative relation between the relative degrees obtains for any triple $F_1 \subseteq F_2 \subseteq F_3$ of field inclusions:

$$[F_3:F_1] = [F_3:F_2][F_2:F_1]. \tag{3}$$

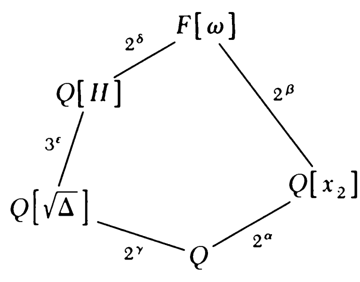
All these facts, including the solution of the cubic equation, are available in [2].

Since $x^3 + px + q = 0$ is assumed to have a rational root x_1, the other two roots, x_2 and x_3, are solutions of a quadratic equation with rational coefficients. We form the field $Q[x_2]$ and since $x_2 + x_3 = -x_1$, we have $x_3 \in Q[x_2]$. Similarly, since $H + K = x_1$, $K \in Q[H]$.

We now ask how the fields $Q[H]$, $Q[\sqrt{\Delta}]$, $F = Q[x_2]$, and $F[\omega]$ (where $\omega = \frac{1}{2}(-1 + i\sqrt{3})$ is a primitive cube root of 1) are related. Since $H^3 = -q/2 + \sqrt{\Delta}$, we have $Q[\sqrt{\Delta}] \subseteq Q[H]$. Clearly $F \subseteq F[\omega]$. Finally the first two of equations (2), regarded as equations for H and K in terms of $\omega, \omega^2, x_1, x_2$, show that

$$H = \frac{\begin{vmatrix} x_1 & 1 \\ x_2 & \omega \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ \omega & \omega^2 \end{vmatrix}} = \frac{\omega x_1 - x_2}{\omega^2 - \omega} \in F[\omega].$$

We can show all the relationships of the various fields in a simple diagram where the lines show containment of one field in another and the numbers represent the relative degree of each field over the one below it. We have $0 \leqslant \alpha, \beta, \gamma, \delta, \varepsilon \leqslant 1$ since the extensions come from equations of the form $z^2 - r = 0$ or $z^3 - s = 0$. An exponent 1 represents a real extension while an exponent 0 means the fields are actually identical.



The multiplicative property of field extensions (3) then gives

$$2^\alpha \cdot 2^\beta = 2^\gamma \cdot 3^\varepsilon \cdot 2^\delta.$$

Obviously, $\varepsilon = 0$, so that $Q[H] = Q[\sqrt{\Delta}]$ and we have $H \in Q[\Delta]$. Hence we have

THEOREM 1. *If the cubic $x^3 + px + q = 0$ has a rational root then $-q/2 + \sqrt{\Delta}$ is the cube of some expression of the form $a + b\sqrt{\Delta}$ where a and b are rational.*

From this we can easily ascertain the precise nature of the roots x_1 and x_2. We set $H = a + b\sqrt{\Delta}$ and then K will be $a - b\sqrt{\Delta}$ (since $3HK = -p$, HK must be rational, which determines K among the three cube roots of $-q/2 - \sqrt{\Delta}$). We also note $\omega + \omega^2 = -1$ and $\omega - \omega^2 = i\sqrt{3}$. Adding the last two of equations (2) we have $x_2 + x_3 = -H - K \in Q$ and subtracting them we have $x_2 - x_3 = i\sqrt{3}(H - K) = i\sqrt{3}(2b\sqrt{\Delta}) = 2b\sqrt{-3\Delta}$. Solving these two equations for x_2 we have $x_2 \in Q[\sqrt{-3\Delta}]$ and, since $x_3 = -x_2 - x_1 \in Q[x_2]$ we have $\sqrt{-3\Delta} \in Q[x_2]$. Hence we have

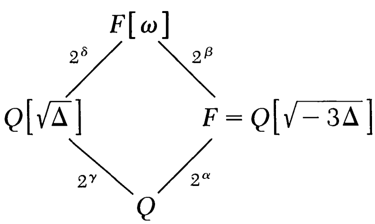
THEOREM 2. a) $Q[x_2] = Q[\sqrt{-3\Delta}]$.
b) *If x_1 is a rational root of $x^3 + px + q = 0$, then the other two roots are in $Q[\sqrt{-3\Delta}]$ and if -3Δ is not a perfect square in Q, then x_2 and $x_3 \notin Q$.*

THEOREM 3. *The equation $x^3 + px + q = 0$ has three rational roots if and only if it has one rational root and -3Δ is a perfect square in Q.*

Proof. The condition is necessary by b) of Theorem 2. Conversely, if -3Δ is a perfect square then by a) of the theorem $Q[x_2] = Q$ so $x_2 \in Q$ and then $x_3 = -x_1 - x_2 \in Q$.

The condition -3Δ is a square in Q is equivalent to $\Delta = -3r^2$ for some rational r. By itself this is not sufficient for three rational roots, as the counterexample $x^3 - 12x + 8 = 0$ shows. Here $-3\Delta = 144$, but there are no rational roots.

Let us revise our previous diagram now that we know $Q[H] = Q[\sqrt{\Delta}]$ and $F = Q[x_2] = Q[\sqrt{-3\Delta}]$. If neither Δ nor -3Δ is a square, then $\alpha = \beta = \gamma = \delta = 1$. This is the "normal case." The exceptional cases occur as follows.



I. Both -3Δ and Δ are squares in Q. But then $-3\Delta^2$ is a square in Q so $\Delta = 0$. This implies $H = K$ so that $x_1 = 2H$, $x_2 = x_3 = -H$, and we have a double root. Since H is rational, in this case $-q/2$ is a perfect cube. Example: $x^3 - 3x - 2 = 0$, $\Delta = 0$.

II. -3Δ a square but Δ not a square in Q. By Theorem 3 we have three rational roots, $\alpha = 0$, $F = Q$ and $\beta = 1$. But since $\gamma + \delta = 1$ and $\gamma = 1$ we have $\delta = 0$. Then $Q[H] = Q[\sqrt{\Delta}] = F[\omega] = Q[\omega]$ (since $F = Q$) and we have $H, K \in Q[\omega] = Q[i\sqrt{3}]$ and again $\Delta = -3r^2$ for rational r. Example: $x^3 - 7x - 6 = 0$, $\Delta = (100/81)(-3)$.

III. -3Δ is not a square and Δ is a square in Q. Then $\sqrt{-3\Delta} = r\sqrt{-3}$ for some rational r and $F = Q[\omega]$. Thus $F[\omega] = F$ and $\beta = 0$. Since $Q[H] = Q[\sqrt{\Delta}]$, in this case H and K are rational numbers. Example: $x^3 - 6x - 9 = 0$, $\Delta = 49/4$, $x_2 = \omega - 1$, $x_3 = -\omega - 2$.

Conversely if the roots lie in $Q[\omega] = Q[i\sqrt{3}]$ but do not all lie in Q, then $Q[\sqrt{-3\Delta}] = F = Q[i\sqrt{3}]$ so Δ is a perfect square. We thus have

THEOREM 4. *Let the cubic $x^3 + px + q = 0$ have one rational root. Then its root field $Q[x_2] = Q[\omega]$ if and only if Δ is a square in Q.*

The condition that $x^3+px+q=0$ have a rational root is essential, for $x^3-6x-6=0$ has $\Delta=1$ but has no rational roots and none of its roots are in $Q[\omega]$.

Final note. All of these results may be proved by elementary means. For example, it is only moderately difficult to prove Theorem 1 by noting that if x_1 is the rational root, then

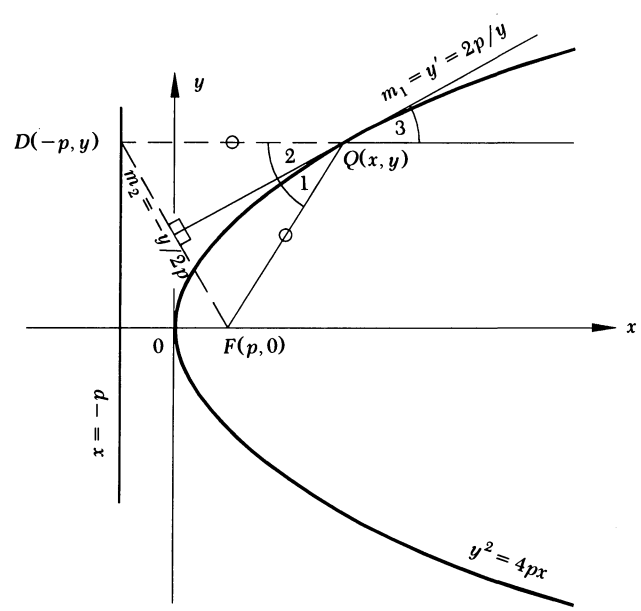
$$\left(\frac{x_1}{2}-\frac{3x_1}{3q+2px_1}\sqrt{\Delta}\right)^3=-\frac{q}{2}+\sqrt{\Delta},$$

which gives an $H\in Q[\sqrt{\Delta}]$. However, this method is unsystematic and makes the results seem to depend on fortuitous algebraic trivialities. The approach through field extensions gives a much better explanation of what is really going on.

REFERENCES

1. Girolamo Cardano, *Ars Magna*, Nuremberg, 1543.
2. A. P. Hillman and G. L. Alexanderson, *A First Undergraduate Course in Abstract Algebra*, 4th edition, Wadsworth Publishing Co., Belmont, CA, 1988.

Proof without Words: The reflection property of the parabola



$$QF=QD \quad \& \quad m_1\cdot m_2=-1 \quad \Rightarrow \quad \measuredangle 1=\measuredangle 2=\measuredangle 3$$

—AYOUB B. AYOUB
PENNSYLVANIA STATE UNIVERSITY
ABINGTON, PA 19001

The condition that $x^3+px+q=0$ have a rational root is essential, for $x^3-6x-6=0$ has $\Delta=1$ but has no rational roots and none of its roots are in $Q[\omega]$.

Final note. All of these results may be proved by elementary means. For example, it is only moderately difficult to prove Theorem 1 by noting that if x_1 is the rational root, then

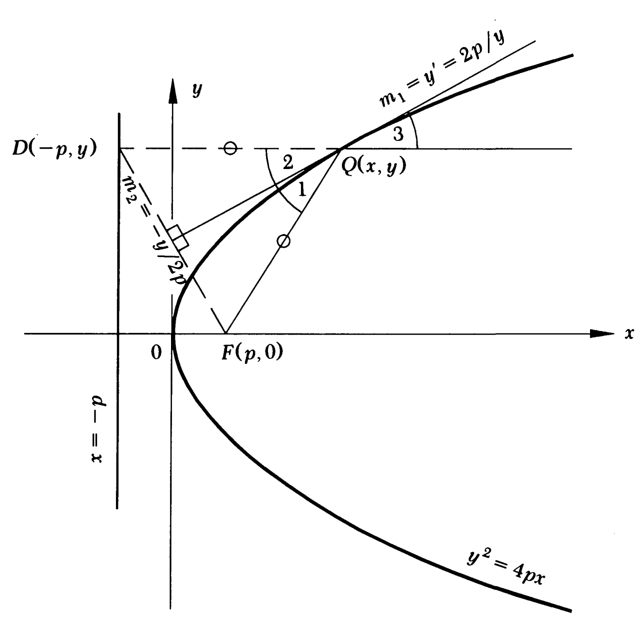
$$\left(\frac{x_1}{2}-\frac{3x_1}{3q+2px_1}\sqrt{\Delta}\right)^3=-\frac{q}{2}+\sqrt{\Delta},$$

which gives an $H\in Q[\sqrt{\Delta}\,]$. However, this method is unsystematic and makes the results seem to depend on fortuitous algebraic trivialities. The approach through field extensions gives a much better explanation of what is really going on.

REFERENCES

1. Girolamo Cardano, *Ars Magna*, Nuremberg, 1543.
2. A. P. Hillman and G. L. Alexanderson, *A First Undergraduate Course in Abstract Algebra*, 4th edition, Wadsworth Publishing Co., Belmont, CA, 1988.

Proof without Words: The reflection property of the parabola



$$QF=QD \quad \& \quad m_1\cdot m_2=-1 \quad \Rightarrow \quad \measuredangle 1=\measuredangle 2=\measuredangle 3$$

—Ayoub B. Ayoub
Pennsylvania State University
Abington, PA 19001

Asymptotic Iteration

VLADIMIR DROBOT
Santa Clara University
Santa Clara, CA 95053

LAWRENCE J. WALLEN
University of Hawaii
Honolulu, HI 96822
and Santa Clara University

1. Introduction Iteration of functions provides an extremely important method for solving equations, indeed, often the only one. Since explicit calculations of the iterates are usually either impossible or uninformative, a great deal of effort has been devoted to obtaining asymptotic formulas for the iterates. These approximations also play a role in stochastic processes (see the beautiful and lucid classic [2]). Indeed, our own interest in these topics arose in probability, albeit, from a more modest problem (see [6]).

In this paper, we will be concerned with asymptotic behavior of the iterates $F(a), F(F(a)), \ldots$ of a real continuous function F near a fixed point. For convenience, we take the fixed point to be zero. The kth iterate of F will be denoted by F_k so that $F_k(x) = F(F_{k-1}(x))$ and $F_0(x) = x$. If F satisfies $0 < F(x) < x$ for $0 < x \leqslant A$, then it is easily seen that $F_k(a) \to 0$ for $0 < a \leqslant A$. The kind of question we consider is exemplified by the question of Pólya-Szegő (see [4], Problem 173; p. 38): About how big is $\sin_k(1)$?

If $F \in C^1$ near $x = 0$ and $|F'(0)| < 1$, then $F_k(a) \to 0$ at least geometrically quickly (i.e., $F_k(a) < Cr^k$ for some $0 < r < 1$) if $|a|$ is small. The more interesting case occurs when $F'(0) = 1$. If, for example, $F(x) = x - Cx^{\alpha} + o(x^{\alpha})$, $\alpha > 1$, $C > 0$, then it is known that

$$F_k(a) \sim \left(\frac{1}{(\alpha - 1)Ck} \right)^{1/(\alpha - 1)}$$

for a near zero (see [3] or [5]). Thus, the answer to the question in the last paragraph is $\sin_k(1) \sim (3/k)^{1/2}$. Throughout, we use the standard notation $\sim$ to mean "asymptotically equal to," and freely avail ourselves of the "little oh" notation.

The case $F(x) = x - Cx^{\alpha} + o(x^{\alpha})$ is discussed in great detail in [1]. Our chief aim is to give an asymptotic formula for a wider class of functions such as $F(x) = x - x^{\alpha}\log|x|$, $\alpha > 1$, or $F(x) = x - \exp(-x^{-\beta})$, $\beta > 0$, where the convergence to the fixed point is very slow. Moreover, our proof is extremely elementary and should be readily accessible to any competent student who's had a traditional advanced calculus course.

2. Some heuristics In this section we give two heuristic arguments that indicate what to expect. We will set $\eta_k = F_k(a)$ when the initial point is unimportant. In the case $F(x) = x - x^{\alpha}$ above, the correct answer is of the form $\xi_k = y(1/k)$ with $y(x) = (Kx)^{\gamma}$ for suitable K and γ. Taking a cue from this, we try to find a smooth function $y(x)$ so that $y(1/k) = \xi_k \approx \eta_k$ (we temporarily use $\approx$ in the usual vague sense "is close to"). Then if $F(x) = x - G(x)$,

$$G(y(1/k)) \approx G(\eta_k) = \eta_k - \eta_{k+1} \approx y(1/k) - y(1/k+1) \approx y'(1/k)/k^2.$$

Thus, we are led to consider the differential equation

$$G(y) = x^2\left(\frac{dy}{dx}\right),$$

which has the solution

$$\frac{1}{x} = \int_{y(x)}^{B} \frac{du}{G(u)}.$$

Setting $x = 1/k$, we see that ξ_k is defined by

$$k = \int_{\xi_k}^{B} \frac{du}{G(u)}. \qquad (*)$$

We can arrive at $(*)$ from a different direction. Consider the usual picture in FIGURE 1 for the iterates. If k is large and F tends to zero slowly, then area$(ABDC) \approx$ 2 area(BCD) or

$$G^2(\eta_k) \approx \int_{\eta_{k+1}}^{\eta_k} G(u)\,du \approx G^2(\eta_k)\int_{\eta_{k+1}}^{\eta_k} \frac{du}{G(u)}.$$

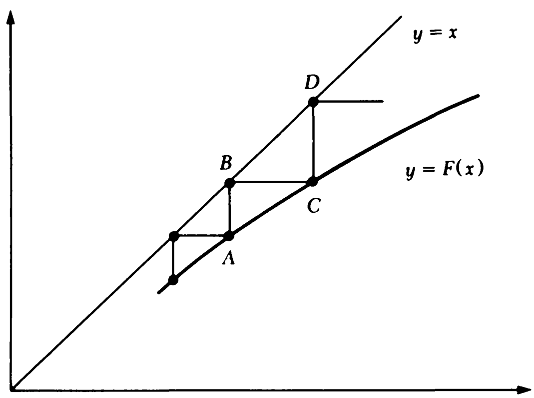


FIGURE 1
$B = (\eta_{k+1}, \eta_{k+1})$, $D = (\eta_k, \eta_k)$, $\overline{CD} = G(\eta_k)$.

Hence

$$1 \approx \int_{\eta_{k+1}}^{\eta_k} \frac{du}{G(u)}, \quad \text{and summing,} \quad k \approx \int_{\eta_k}^{\eta_0} \frac{du}{G(u)}.$$

By taking ξ_k to make the last relation exact, we arrive again at $(*)$.

There are other heuristic arguments useful in arriving at $(*)$ that use the notion of "continuous iteration" and certain equations which arise there, e.g., Abel's equation. Since this direction is less elementary, we will not include them here.

The formula $(*)$ turns out to be wrong in the case when $F(x) \to 0$ very quickly. For example, if $F(x) = x - x|\log x|^{-1}$, an easy computation gives $\xi_k \sim \exp(-\sqrt{2k})$, which turns out to be way off the mark. Thus, in order to assert the validity of the relation $\eta_k \sim \xi_k$ we are going to have to insure that $F(x) \to 0$ fairly slowly.

3. A theorem and some applications

THEOREM. *Let* $F(x) = x - G(x)$, $0 \leqslant x \leqslant A$. *Assume that* $G(x)$ *is* C^1, $G(0) = G'(0) = 0$ *and that* G *is strictly increasing. Define a function*

$$H(x) = \int_x^A \frac{du}{G(u)}$$

and let ξ_k *be determined by* $H(\xi_k) = k$. *Suppose also that for each* $\mu > 1$

$$\limsup_{x \to 0} \frac{H(\mu x)}{H(x)} < 1.$$

Then $\xi_k \sim \eta_k = F_k(A)$.

Remark. The last hypothesis is one way of saying that $G(x)$ tends to zero quickly, or equivalently, that $F(x)$ tends to zero slowly. It is not satisfied by the function $G(x) = x|\log x|^{-1}$ mentioned above. Also $0 < G(x) < x$ and $0 < F(x) < x$ near zero and we will assume that this holds for all $0 < x \leqslant A$. Finally, the upper limit in the integral is clearly immaterial.

Proof. The proof of the theorem is a variant of the second heuristic argument, but is based on the different, more convenient picture in FIGURE 2. The area of the inscribed rectangle with vertices $(x,0)$, $(F(x),0)$, R, and S is 1, as can be easily checked using $F(x) = x - G(x)$. Let $\lambda(x)$ be the area above this rectangle and below the graph of $1/G(u)$. Since $H(\xi_k) = k$, we have

$$H(\eta_k) = \int_{\eta_k}^{\eta_0} \frac{du}{G(u)} = k + \sum_{j=0}^{k-1} \lambda(\eta_j) = H(\xi_k) + \Lambda(k),$$

where $\Lambda(k) = \sum_0^{k-1} \lambda(\eta_j)$. The proof consists of showing that $\Lambda(k) = o(k)$, which implies that $H(\eta_k) \sim H(\xi_k)$, and then showing that this, in turn, implies $\eta_k \sim \xi_k$.

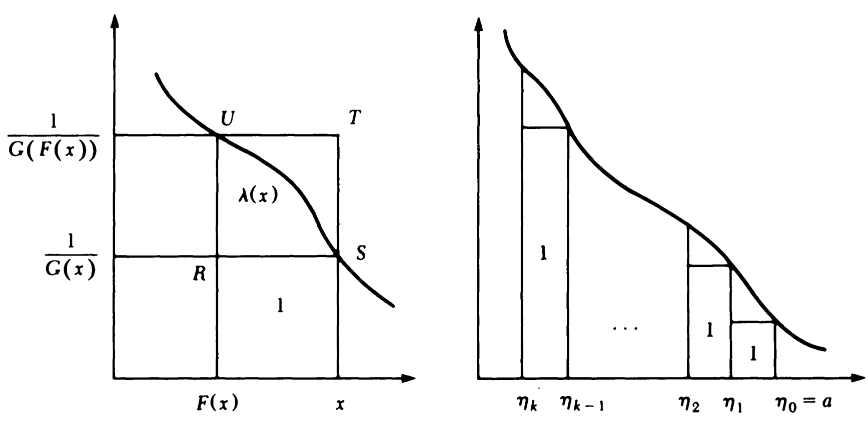


FIGURE 2
The graph in both cases is that of $\frac{1}{G(u)}$.

Now

$$\lambda(x) < \text{area}(RSTU) = (x - F(x))\left[\frac{1}{G(F(x))} - \frac{1}{G(x)}\right]$$
$$= G(x)\left[\frac{1}{G(x - G(x))} - \frac{1}{G(x)}\right]$$
$$= \frac{G(x) - G(x - G(x))}{G(x - G(x))}.$$

Writing $G(x - G(x)) = G(x) - G'(\theta)G(x)$, $x - G(x) < \theta < x$, this last quotient is equal to $G'(\theta)[1 - G'(\theta)]^{-1} = o(1)$ as $x \to 0$. Thus, $\lambda(\eta_k) \to 0$ and so $k^{-1}(\sum_{j=0}^{k-1}\lambda(\eta_j)) \to 0$, or $\Lambda(k) = o(k)$. Hence $H(\eta_k) \sim H(\xi_k)$.

From FIGURE 2, we see that $\eta_k < \xi_k$ since $H(\eta_k) > k = H(\xi_k)$. If the relation $\eta_k \sim \xi_k$ does not hold, then for some $\mu > 1$, $\mu\eta_k \leqslant \xi_k$ for an infinite sequence S of k's. Using the last assumption of the theorem, pick $\delta > 0$ so that $H(\mu x)[H(x)]^{-1} \leqslant 1 - \delta$ for $x < x_o$. Now, for $k \in S$

$$H(\eta_k) = \int_{\eta_k}^{\mu\eta_k}\frac{du}{G(u)} + \int_{\mu\eta_k}^{A}\frac{du}{G(u)} \geqslant \int_{\eta_k}^{\mu\eta_k}\frac{du}{G(u)} + \int_{\xi_k}^{A}\frac{du}{G(u)}$$
$$= H(\eta_k) - H(\mu\eta_k) + H(\xi_k).$$

Consequently, if $\eta_k < x_o$, $1 - \delta \geqslant H(\xi_k)[H(\eta_k)]^{-1}$, contradicting the fact that $H(\xi_k) \sim H(\eta_k)$.

We can now easily dispose of the questions raised in the introduction. If $G(x) = Mx^\alpha \log(x^{-1})$ with $\alpha > 1$, $M > 0$, then

$$H(x) = M^{-1}\int_x^A \frac{du}{u^\alpha \log(u^{-1})} = M^{-1}\int_c^{\log(x^{-1})} y^{-1}e^{(\alpha-1)y}\,dy \sim M^{-1}\frac{x^{-(\alpha-1)}}{\log(x^{-(\alpha-1)})},$$

the last step following from an integration by parts. It follows that G satisfies the conditions of the theorem. Since the solution $v = v(t)$ of $t = v/\log v$ satisfies $v \sim t\log t$ as $t \to \infty$, we get

$$F_k(A) = \eta_k \sim \xi_k \sim \left[\frac{1}{Mk\log k}\right]^{1/(\alpha-1)}$$

If $G(x) = \exp(-x^{-\beta})$, $\beta > 0$, another routine calculation gives

$$H(x) \sim \beta^{-1}x^{1+\beta}\exp(x^{-\beta}),$$

from which we easily deduce that

$$F_k(A) = \eta_k \sim \left(\frac{1}{\log k}\right)^{1/\beta}.$$

We give one final application by addressing the question: When does $\sum_{k=1}^{\infty}\eta_k$ converge? Here is an elementary argument that gives some information. If $F(x)$ is concave and increasing with $0 < F(x) < x$, then

$$\eta_k = \int_0^a F_k'(x)\,dx = \int_0^a \prod_{j=0}^{k-1} F'(F_j(x))\,dx \geqslant \int_0^a (F'(x))^k\,dx$$

and so

$$\sum_{k=0}^{\infty} \eta_k \geqslant \int_0^a \frac{dx}{1-F'(x)}.$$

In case F satisfies the conditions of our theorem, we get a complete answer as follows. Let K be the function on $0 \leqslant u < \infty$ inverse to H so that $K(k) = \xi_k$. Then $\Sigma\eta_k$ converges or diverges with $\Sigma K(k) = \Sigma\xi_k$. Since

$$\int_0^{\infty} K(u)\,du = \int_0^a x(-H'(x))\,dx = \int_0^a \frac{x}{G(x)}\,dx = \int_0^a \left(1 - \frac{F(x)}{x}\right)^{-1} dx,$$

we see that $\Sigma\eta_k$ is finite exactly when the last integral is finite.

REFERENCES

1. N. G. de Bruijn, *Asymptotic Methods in Analysis*, John Wiley and Sons, Inc., New York, 1961.
2. T. E. Harris, *The Theory of Branching Processes*, Springer-Verlag, New York, 1963.
3. A. M. Ostrowski, *Solutions of Equations in Euclidean and Banach Spaces*, Academic Press, New York, 1973.
4. G. Pólya and G. Szegő, *Problems and Theorems in Analysis*, Vol. 1, Springer-Verlag, New York, 1972.
5. G. Szekeres, Regular iterations of real and complex functions, *Acta Math.* 100 (1958), 203–258.
6. L. J. Wallen, Modified iterations and probability, *Amer. Math. Monthly* 92 (1985), 481–485.

The Kuratowski Closure-Complement Problem

JAMES H. FIFE
Ursinus College
Collegeville, PA 19426

A famous problem in point-set topology is the Kuratowski closure-complement problem. (See [1], [3], and [4].) The problem is to show that, starting with a subset A of a topological space X, and alternately taking closures and complements, one never obtains more than 14 different sets, and then to find an example of a subset of the real numbers for which one obtains exactly 14 different sets. While the second part of this problem is within the range of most undergraduate topology or analysis students, the first part seems to be extremely difficult. It appears that the only published solution is Kuratowski's original proof [2], in French and in a journal not likely to be in most undergraduate libraries. Since there is no readily available solution in English for students, we are supplying the following proof, similar to, though not identical with, Kuratowski's original.

THEOREM. *Let X be a topological space, and let $A \subset X$. By alternately taking closures and complements of A, no more than 14 different sets are generated.*

We shall write A^- for the closure of A and A^c for the complement of A. We shall also write A^i for the interior of A. Note that $A^{--} = A^-$ and $A^{cc} = A$. We shall begin with a couple of lemmas.

and so

$$\sum_{k=0}^{\infty} \eta_k \geqslant \int_0^a \frac{dx}{1-F'(x)}.$$

In case F satisfies the conditions of our theorem, we get a complete answer as follows. Let K be the function on $0 \leqslant u < \infty$ inverse to H so that $K(k) = \xi_k$. Then $\Sigma \eta_k$ converges or diverges with $\Sigma K(k) = \Sigma \xi_k$. Since

$$\int_0^{\infty} K(u)\, du = \int_0^a x(-H'(x))\, dx = \int_0^a \frac{x}{G(x)}\, dx = \int_0^a \left(1 - \frac{F(x)}{x}\right)^{-1} dx,$$

we see that $\Sigma \eta_k$ is finite exactly when the last integral is finite.

REFERENCES

1. N. G. de Bruijn, *Asymptotic Methods in Analysis*, John Wiley and Sons, Inc., New York, 1961.
2. T. E. Harris, *The Theory of Branching Processes*, Springer-Verlag, New York, 1963.
3. A. M. Ostrowski, *Solutions of Equations in Euclidean and Banach Spaces*, Academic Press, New York, 1973.
4. G. Pólya and G. Szegő, *Problems and Theorems in Analysis*, Vol. 1, Springer-Verlag, New York, 1972.
5. G. Szekeres, Regular iterations of real and complex functions, *Acta Math.* 100 (1958), 203–258.
6. L. J. Wallen, Modified iterations and probability, *Amer. Math. Monthly* 92 (1985), 481–485.

The Kuratowski Closure-Complement Problem

JAMES H. FIFE
Ursinus College
Collegeville, PA 19426

A famous problem in point-set topology is the Kuratowski closure-complement problem. (See [1], [3], and [4].) The problem is to show that, starting with a subset A of a topological space X, and alternately taking closures and complements, one never obtains more than 14 different sets, and then to find an example of a subset of the real numbers for which one obtains exactly 14 different sets. While the second part of this problem is within the range of most undergraduate topology or analysis students, the first part seems to be extremely difficult. It appears that the only published solution is Kuratowski's original proof [2], in French and in a journal not likely to be in most undergraduate libraries. Since there is no readily available solution in English for students, we are supplying the following proof, similar to, though not identical with, Kuratowski's original.

THEOREM. *Let X be a topological space, and let $A \subset X$. By alternately taking closures and complements of A, no more than 14 different sets are generated.*

We shall write A^- for the closure of A and A^c for the complement of A. We shall also write A^i for the interior of A. Note that $A^{--} = A^-$ and $A^{cc} = A$. We shall begin with a couple of lemmas.

LEMMA 1. *Let X be a topological space, and let $A \subset X$.*

(a) $$A^{-c} = A^{ci}$$

(b) $$A^{c-} = A^{ic}.$$

Proof. Suppose $x \in A^{-c}$. Then $x \notin A^{-}$. Since $y \in A^{-}$ if and only if every neighborhood of y intersects A, it follows that there is a neighborhood U of x such that U does not intersect A; that is, $U \subset A^{c}$. The existence of such a U shows that $x \in A^{ci}$. Thus $A^{-c} \subset A^{ci}$. Since each of these steps is reversible, we also have $A^{-c} \supset A^{ci}$. Thus $A^{-c} = A^{ci}$.

This proves part (a). The proof of (b) is similar.

LEMMA 2. *Let X be a topological space, and let $A \subset X$.*

(a) *If A is open, then $A \subset A^{-i}$.*

(b) *If A is closed, then $A \supset A^{i-}$.*

Proof. Suppose A is open. Since $A \subset A^{-}$, and A^{-i} is the union of all open sets $U \subset A^{-}$, it follows that $A \subset A^{-i}$.

This proves part (a). The proof of (b) is similar.

Remark. $A = (0,1) \cup (1,2)$ shows that equality does not hold in part (a), and $A = (0,1) \cup \{2\}$ shows that containment does not hold if A is not open. Similar examples apply to part (b).

Proof of theorem. Part (a) of Lemma 2 states that, if A is open, then

$$A \subset A^{-i}.$$

Taking the closure of both sides, we have

$$A^{-} \subset A^{-i-}.$$

But for any A, A^{-} is closed, so it follows from part (b) of Lemma 2, applied to A^{-}, that

$$A^{-} \supset A^{-i-}.$$

Thus we have

$$A^{-} = A^{-i-} \tag{1}$$

if A is open. Similarly

$$A^{i} = A^{i-i} \tag{2}$$

if A is closed.

In particular, if A is any subset of X, then A^{i} is open. So it follows from (1), applied to A^{i}, that

$$A^{i-} = A^{i-i-}. \tag{3}$$

Similarly, A^{-} is closed, so it follows from (2) that

$$A^{-i} = A^{-i-i}. \tag{4}$$

Now let A be any subset of X. Then

$$A^{c-c-} = A^{icc-} \quad \text{by part (b) of Lemma 1}$$
$$= A^{i-} \quad \text{since } A^{cc} = A.$$

Thus

$$A^{c-c-c-c-} = A^{i-i-}$$
$$= A^{i-} \text{ by (3)}$$
$$= A^{c-c-},$$

or

$$A^{c-c-c-c-} = A^{c-c-}. \tag{5}$$

Similarly, $A^{-c-c-c-c} = A^{-c-c}$. Taking the complement of both sides, we have

$$A^{-c-c-c-cc} = A^{-c-cc},$$

or

$$A^{-c-c-c-} = A^{-c-}. \tag{6}$$

Thus starting with A, we obtain the following 14 sets:

1. A
2. A^c
3. A^{c-}
4. A^{c-c}
5. A^{c-c-}
6. $A^{c-c-c} = A^{-c-}$
7. A^{c-c-c-}
8. $A^{c-c-c-c}$
   [$A^{c-c-c-c-} = A^{c-c-}$ by (5)]
9. A^-
10. A^{-c}
11. A^{-c-}
12. A^{-c-c}
13. A^{-c-c-}
14. A^{-c-c-c}
   [$A^{-c-c-c-} = A^{-c-}$ by (6).]

This completes the proof.

Note that if, in addition to taking complements and closures of A, one also takes *interiors* of A, no additional sets are generated, because, as a corollary of Lemma 1, $A^i = A^{cci} = A^{c-c}$. Note also that this theorem is essentially a theorem about the monoid generated by c, $-$, and i, subject to certain relations. That is, the theorem can be rephrased as follows:

Let G be the monoid generated by c, k, and i, subject to the relations

$$c^2 = 1 \qquad kc = ci \qquad ik = (ik)^2$$
$$i^2 = i \qquad ck = ic \qquad ki = (ki)^2$$
$$k^2 = k.$$

Then G has 14 elements.

REFERENCES

1. John L. Kelly, *General Topology*, Van Nostrand Reinhold Co., Inc., Princeton, NJ, 1955.
2. Casimir Kuratowski, Sur l'opération a de l'analysis situs, *Fund. Math.* 3 (1922), 196.
3. ______, *Topologie I*, Warsaw, 1948.
4. James R. Munkres, *Topology: A First Course*, Prentice-Hall, Englewood Cliffs, NJ, 1975.

Majorization and the Birthday Inequality

M. LAWRENCE CLEVENSON
WILLIAM WATKINS
California State University
Northridge, CA 91330

Introduction If there are k people in a room, what is the probability that at least two of them have the same birthday? Intuitively, people guess that the answer is $k/365$ or close to it [4]. Of course the probability of a match is

$$1-(365)(364)\cdots(365-k+1)/365^k,$$

which is greater than 0.5 even if there are only 23 people in the room. Probability instructors are fond of demonstrating this fact in class by asking the students to announce their birthdays until a match is discovered. The authors are courageous enough to try the demonstration in classes with 30 or more students so that the probability of a match is at least 0.706.

Recently, however, we got worried. The probabilities given above are based on the assumption that a randomly chosen individual is just as likely to have a birthday on, say, October 1 as on January 10. In other words, the assumption is that

$$p_i = 1/365,$$

for $i=1,\dots,365$, where p_i is the probability that a randomly chosen individual has a birthday on the ith day of the year. Since some births are scheduled, this assumption of equally likely birthdays is questionable. So, the probability of a match with, say, 30 people in the room is not necessarily 0.706. Could it be smaller? Should we be less courageous in our classroom demonstrations? The answer is no. If the distribution of birthdays is not uniform, then the probability of a match is at least as large as it is when the birthdays are uniformly distributed throughout the year. We call this fact the birthday inequality.

It isn't new. Bloom [1] and Rust [6] give proofs using Lagrange multipliers and Munford [5] gives one using elementary symmetric functions. Our purpose is to strengthen the birthday inequality and to place it in its natural setting—the theory of majorization and Schur-convexity. The stronger result appears in Marshall and Olkin's book on majorization [3, p. 305] as a corollary to a much more general theorem. Our treatment is elementary.

The birthday inequality Let the n-tuple $\mathbf{p}=(p_1,\dots,p_n)$ be any probability vector of birthdays for the $n=365$ days of the year. Given $\mathbf{p}$, let $P_k(\mathbf{p})$ denote the probability of at least one match among k people and let $Q_k(\mathbf{p})=1-P_k(\mathbf{p})$ be the probability of the complementary event that all k birthdays are different. We want to prove $P_k(\mathbf{p})\geqslant P_k(\mathbf{u})$, or equivalently

$$Q_k(\mathbf{p})\leqslant Q_k(\mathbf{u}), \tag{1}$$

where $\mathbf{u}=(1/n,\dots,1/n)$ is the uniform distribution of birthdays.

We need a formula for $Q_k(\mathbf{p})$. Given k people and an ordered selection $i_1, \ldots, i_k$ of k days of the year, the probability that person j is born on day i_j, for $j = 1, \ldots, k$ is $p_{i_1} \cdots p_{i_k}$. It follows that

$$Q_k(\mathbf{p}) = \sum p_{i_1} \cdots p_{i_k}, \tag{2}$$

where the sum is taken over all sequences $i_1, \ldots, i_k$ of distinct integers from 1 to n. This sum is easy to compute for the uniform distribution. There are $(365)(364) \cdots (365 - k + 1)$ ways to pick a sequence of k distinct integers from $1, \ldots, 365$. So the probability of no match is given by $Q_k(\mathbf{u}) = (365)(364) \cdots (365 - k + 1)/365^k$, as we saw earlier.

The proof of inequality (1) requires a slight reformulation of formula (2) in terms of elementary symmetric functions. The *kth elementary symmetric function* of $\mathbf{p} = (p_1, \ldots, p_n)$ is defined by

$$E_k(\mathbf{p}) = \sum p_{i_1} \cdots p_{i_k},$$

where the sum is taken over all strictly increasing sequences $i_1, \ldots, i_k$ of integers from 1 to n. Since $Q_k(\mathbf{p}) = k!\,E_k(\mathbf{p})$, it suffices to prove that

$$E_k(\mathbf{p}) \leqslant E_k(\mathbf{u}) \tag{3}$$

instead of the original birthday inequality (1).

Proof of the birthday inequality One of the ideas involved in the proof is that of a *T-transform*. Given an n-tuple, say $\mathbf{p} = (.28, .16, .41, .11, .04)$, pick two coordinates, say $p_1 = .28$ and $p_2 = .16$. A T-transform has the following action on $\mathbf{p}$:

$$(.28, .16, .41, .11, .04) \to (.28 - d, .16 + d, .41, .11, .04),$$

where d is a positive number satisfying $d \leqslant |p_1 - p_2|$ that must be subtracted from the larger of the two coordinates and added to the smaller. If we choose $d = .08$, then the corresponding T-transform sends $\mathbf{p}$ to $(.20, .24, .41, .11, .04)$. Only two of the coordinates of $\mathbf{p}$ are changed and they get closer together. We might say that $(.20, .24, .41, .11, .04)$ is more uniform or less spread out than $(.28, .16, .41, .11, .04)$—an idea that we will develop in the next section. The T-transform does not change the sum of the coordinates of $\mathbf{p}$.

An appropriate sequence of T-transforms can change any probability vector $\mathbf{p}$ into the uniform probability vector $\mathbf{u}$. To see this observe that if $\mathbf{p} \neq \mathbf{u}$ then $\mathbf{p}$ has a pair of coordinates p_i, p_j, satisfying $p_i > 1/n > p_j$. Let T be the T-transform that subtracts $d = p_i - 1/n$ from the ith coordinate of $\mathbf{p}$ and adds d to the jth coordinate. Then the ith coordinate of $T\mathbf{p}$ is $1/n$. In this way $\mathbf{p}$ can be transformed by a sequence of T-transforms to $\mathbf{u}$. In our example, four T-transforms are needed to get from $\mathbf{p}$ to $\mathbf{u}$:

$$\begin{aligned}(.28, .16, .41, .11, .04) &\to (.20, .24, .41, .11, .04)\\ &\to (.20, .20, .41, .15, .04)\\ &\to (.20, .20, .20, .15, .25)\\ &\to (.20, .20, .20, .20, .20).\end{aligned}$$

Why introduce the T-transform? Because it increases the value of the kth elementary symmetric function. That is, if $\mathbf{p}$ is a probability vector and T is a T-transform, then

$$E_k(\mathbf{p}) \leqslant E_k(T\mathbf{p}). \tag{4}$$

This is just what we need to prove the birthday inequality. If $\mathbf{p} \to \mathbf{q} \to \mathbf{r} \to \cdots \to \mathbf{u}$ is a sequence of T-transforms that takes $\mathbf{p}$ to the uniform distribution $\mathbf{u}$, then from (4) we have

$$E_k(\mathbf{p}) \leqslant E_k(\mathbf{q}) \leqslant E_k(\mathbf{r}) \leqslant \cdots \leqslant E_k(\mathbf{u})$$

and inequality (3) will be proved. All that remains in the proof of the birthday inequality is to show (4). We accomplish this using two properties of the elementary symmetric functions.

First, elementary symmetric functions are symmetric. That is, a permutation of the coordinates of $\mathbf{p}$ does not change the value of the elementary symmetric function. Thus to prove inequality (4), we may assume that $\mathbf{p} = (p_1, \dots, p_n)$ with $p_1 > p_2$ and that the T-transform changes only the first two coordinates of $\mathbf{p}$. So suppose $T\mathbf{p} = (p_1 - d, p_2 + d, p_3, \dots, p_n)$. The second property of the elementary symmetric functions is that they occur as the coefficients of the polynomial $(x + p_1)(x + p_2) \cdots (x + p_n)$. That is,

$$(x + p_1) \cdots (x + p_n) = x^n + E_1(\mathbf{p})x^{n-1} + \cdots + E_k(\mathbf{p})x^{n-k} + \cdots + E_n(\mathbf{p}).$$

Only the first two factors of the polynomials

$$(x + p_1)(x + p_2)(x + p_3) \cdots (x + p_n) \tag{5}$$

and

$$(x + p_1 - d)(x + p_2 + d)(x + p_3) \cdots (x + p_n) \tag{6}$$

differ. Examine the coefficients of the quadratics

$$(x + p_1)(x + p_2) = x^2 + (p_1 + p_2)x + p_1 p_2 \tag{7}$$

and

$$(x + p_1 - d)(x + p_2 + d) = x^2 + (p_1 + p_2)x + \left(p_1 p_2 + (p_1 - p_2)d - d^2\right). \tag{8}$$

Both coefficients of x^2 equal 1. The coefficients of x are also the same but the constant term in (7) is less than or equal to the constant term in (8) because $0 < d \leqslant p_1 - p_2$. Since the p_i are nonnegative, every coefficient of polynomial (5) is less than or equal to the corresponding coefficient in (6). Specifically, $E_k(\mathbf{p}) \leqslant E_k(T\mathbf{p})$. This completes the proof of (4) and the birthday inequality.

We have proved more than the birthday inequality. Namely, if $\mathbf{p}$ and $\mathbf{q}$ are probability vectors and there is a sequence of T-transforms changing $\mathbf{p}$ to $\mathbf{q}$, then $P_k(\mathbf{q}) \leqslant P_k(\mathbf{p})$. But for a given pair of probability vectors, it may not be easy to tell if one of them can be obtained by applying a sequence of T-transforms to the other one. In the next section we examine the conditions under which an arbitrary n-tuple $\mathbf{y}$ can be obtained from an n-tuple $\mathbf{x}$ by a sequence of T-transforms.

Majorization and Schur-convexity Let $\mathbf{x}$ and $\mathbf{y}$ be any two real n-tuples. How can we tell if there is a sequence of T-transforms that change $\mathbf{x}$ to $\mathbf{y}$? The following theorem [3, p. 7] provides a simple answer in terms of partial sums of the largest coordinates of the vectors $\mathbf{x}$ and $\mathbf{y}$. We omit the proof. The coordinates for any $\mathbf{z} = (z_1, \dots, z_n)$, arranged in nonincreasing order will be denoted by $z_{[1]} \geqslant z_{[2]} \geqslant \cdots \geqslant z_{[n]}$.

THEOREM. *Let* $\mathbf{x} = (x_1, \dots, x_n)$ *and* $\mathbf{y} = (y_1, \dots, y_n)$ *be real n-tuples. There exists a sequence of T-transforms that changes* x *to* y *if and only if*

$$x_{[1]} + \cdots + x_{[r]} \geqslant y_{[1]} + \cdots + y_{[r]}, \tag{9}$$

for all $r = 1, \dots, n$, *and*

$$x_1 + \cdots + x_n = y_1 + \cdots + y_n. \tag{10}$$

These conditions are very easy to check for any given pair of n-tuples. For example, (9) and (10) hold for the vectors $\mathbf{x} = (.28, .16, .41, .11, .04)$ and $\mathbf{y} = (.20, .20, .20, .15, .25)$. Thus the theorem tells us what we have already verified—there is a sequence of T-transforms taking x to y. If (9) and (10) hold, we say that x *majorizes* y and we write $\mathbf{x} \gg \mathbf{y}$. Intuitively, x is more spread out than y or equivalently, y is more uniform than x. Equation (10) means that we can compare (via majorization) only those n-tuples whose coordinate sums are equal. The largest and smallest n-tuples with nonnegative coordinates and given coordinate sum S are $(S, 0, \dots, 0)$ and $(S/n, \dots, S/n)$, respectively. That is, if each $x_i \geqslant 0$ and $x_1 + \cdots + x_n = S$, then

$$(S, 0, \dots, 0) \gg (x_1, \dots, x_n) \gg (S/n, \dots, S/n).$$

In the case of probability vectors, the uniform distribution $(1/n, \dots, 1/n)$ is majorized by all other probability vectors.

We turn now to the definition of Schur-convex and Schur-concave functions. A real-valued function $F(\mathbf{x})$ of n real variables $\mathbf{x} = (x_1, \dots, x_n)$ is *Schur-convex* if $\mathbf{x} \gg \mathbf{y}$ implies $F(\mathbf{x}) \geqslant F(\mathbf{y})$ and *Schur-concave* if $\mathbf{x} \gg \mathbf{y}$ implies $F(\mathbf{x}) \leqslant F(\mathbf{y})$. Equivalently, $F(\mathbf{x})$ is Schur-convex (Schur-concave) if $F(\mathbf{x}) \geqslant F(T\mathbf{x})$ ($F(\mathbf{x}) \leqslant F(T\mathbf{x})$), for all T-transforms. Perhaps Schur-increasing and Schur-decreasing would be better terms, but the names convex and concave have been in use for a long time. From the definition we see that among all n-tuples with nonnegative coordinates and a given coordinate sum S, a Schur-convex function takes its maximum value at $(S, 0, \dots, 0)$ and its minimum value at $(S/n, \dots, S/n)$. In the case of a probability vector, a Schur-convex function takes its maximum value at $(1, 0, \dots, 0)$ and its minimum value at the uniform probability vector $\mathbf{u} = (1/n, \dots, 1/n)$. We have shown that $P_k(\mathbf{p})$ is a Schur-convex function of $\mathbf{p}$. Thus the probability of matching birthdays is least when the probability vector is $\mathbf{u}$ and greatest when everyone is born on the same day of the year. For a Schur-concave function, the maximum and minimum are reversed.

Many standard inequalities involve Schur-convex or Schur-concave functions F and have the form

$$F(x_1, \dots, x_n) \geqslant F(S/n, \dots, S/n)$$

or

$$F(x_1, \dots, x_n) \leqslant F(S/n, \dots, S/n).$$

The arithmetic-geometric mean inequality is an example. For nonnegative numbers $x_1, \dots, x_n$, the arithmetic-geometric mean inequality can be written in the form

$$x_1 \dots x_n \leqslant (S/n)^n.$$

Recasting this inequality in terms of the nth elementary symmetric function $E_n(x_1, \dots, x_n) = x_1 \dots x_n$ we get

$$E_n(x_1,\ldots,x_n) \leqslant E_n(S/n,\ldots,S/n).$$

In the proof of the birthday inequality, we showed that the elementary symmetric functions $E_k(\mathbf{p})$ are Schur-concave, at least for probability distributions $\mathbf{p}$. In fact, the same proof shows that the elementary symmetric functions are Schur-concave on the set of all n-tuples with nonnegative coordinates; they need not sum to 1. In particular, the function E_n is Schur-concave and the arithmetic-geometric mean inequality is equivalent to the fact that E_n attains its maximum value at $(S/n,\ldots,S/n)$.

Now we return to probability and give another example of a function of a probability vector that is Schur-convex and thus obtains its minimum value at the uniform probability distribution $\mathbf{u}$.

The collector's inequality There are n distinct baseball cards; one of these is included in each package of bubble gum. The collector's goal is to obtain at least one copy of each card. Unfortunately, all selections are made blindly. (You have to buy the bubble gum before you can open the package and see which card is inside.) The collector's problem is this: What is the average (expected) number of packages required in order to obtain a complete collection of all n baseball cards?

First, assume that the cards are uniformly distributed in the gum packages. Then the average number of packages required to collect a complete set is given by,

$$A(\mathbf{u}) = n/n + n/(n-1) + \cdots + n/2 + n/1. \tag{11}$$

This well-known formula appears in Feller's book [**2**, p. 225]. The proof depends on this intuitive result: If p is the probability of success in a sequence of Bernoulli trials, then the average number of trials required to obtain a success is $1/p$.

But what if the cards are not distributed uniformly in the gum packages? Then the average number of packages $A(\mathbf{p})$ required to collect a complete set depends on the probability vector $\mathbf{p} = (p_1,\ldots,p_n)$, where p_i is the probability that a randomly chosen gum package contains card i. The result we wish to point out is that $A(\mathbf{p})$ is a Schur-convex function of the probability vector $\mathbf{p}$. That is, if $\mathbf{p} \gg \mathbf{q}$, then $A(\mathbf{p}) \geqslant A(\mathbf{q})$. Thus, the minimum value of $A(\mathbf{p})$ occurs when $\mathbf{p}$ is the uniform distribution $\mathbf{u} = (1/n,\ldots,1/n)$, i.e., when each of the cards is just as likely to occur in a package as any other card. The proof that $A(\mathbf{p})$ is Schur-convex follows from a theorem in Marshall and Olkin [**3**, pp. 297, 306]. We present a simple proof that $A(\mathbf{p})$ is Schur-convex in the case $n = 2$. In this case there are only two cards to collect, say Aaron and Ruth. Suppose these cards occur with probabilities p_1 and p_2, respectively. If we get Aaron in the first package, then (by the intuitive result above) the expected number of additional packages required to get Ruth is $1/p_2$. So in this case we expect to buy a total of $1 + 1/p_2$ packages. Likewise, if we get Ruth first, then we expect to buy a total of $1 + 1/p_1$ packages. Thus

$$\begin{aligned} A(p_1,p_2) &= p_1(1+1/p_2) + p_2(1+1/p_1) \\ &= 1 + p_1/p_2 + p_2/p_1. \end{aligned} \tag{12}$$

Equipped with formula (12) for $A(\mathbf{p})$, we proceed to show that $A(\mathbf{p})$ is Schur-convex. This amounts to showing that $A(1-p_2,p_2)$ is a decreasing function in p_2, for p_2 in the interval $[0,1/2]$. (By symmetry, we may assume that $0 \leqslant p_2 \leqslant 1/2$.) But

$$\begin{aligned} A(1-p_2,p_2) &= 1 + (1-p_2)/p_2 + p_2/(1-p_2) \\ &= 1/(p_2(1-p_2)) - 1. \end{aligned}$$

The quadratic $p_2(1-p_2)$ increases on the interval $[0,1/2]$, so $A(1-p_2, p_2)$ decreases on the same interval. Thus $A(\mathbf{p})$ is Schur-convex for $n=2$.

We have given two examples of a function in several variables with constant sum that attains its maximum or minimum value at the point where all the variables are equal. When you encounter such an inequality, you should suspect that a stronger version may be true. The function might also be Schur-convex or Schur-concave. For a superb account of the history, theory, and applications of majorization see Marshall and Olkin's definitive work [3].

REFERENCES

1. D. M. Bloom, A birthday problem, *Amer. Math. Monthly* 80 (1973), 1141–2.
2. William Feller, *An Introduction to Probability Theory and Its Applications*, Vol. 1, 3rd edition, John Wiley & Sons, New York, 1970.
3. Albert W. Marshall and Ingram Olkin, *Inequalities: Theory of Majorization and Its Applications*, Academic Press, New York, 1979.
4. Frederick Mosteller, *Fifty Challenging Problems in Probability with Solutions*, Addison-Wesley, Reading, MA, 1965.
5. A. G. Munford, A note on the uniformity assumption in the birthday problem, *The Amer. Statist.* 31 (1977), 119.
6. Philip F. Rust, The effect of leap years and seasonal trends on the birthday problem, *The Amer. Statist.* 30 (1976), 197–8.

Monte Carlo Simulation of Infinite Series

FREDERICK SOLOMON
Warren Wilson College
Swannanoa, NC 28778

Let c be a real number. A *Monte Carlo simulation* of c consists of these steps: First, a random experiment is devised and a random variable X is defined for the experiment such that the expectation of X satisfies $c=E(X)$. Second, the random experiment is performed a large number, K of times; let X_i denote the value of X on the ith experiment. By the Strong Law of Large Numbers,

$$c=E(X_i)=\lim_{K\to\infty}\frac{X_1+X_2+\cdots+X_K}{K}$$

with probability 1. Consequently, for large K, c "should be" approximately $(X_1+X_2+\cdots+X_K)/K$. This ratio is then the Monte Carlo estimate of c.

This method also covers the case in which the constant c is represented as the *probability of an event* A rather than directly as the expectation of a random variable. Namely if $c=P(A)$, then perform the random experiment through which event A is defined and define the random variable X by

$$X=\begin{cases}1, & \text{if } A \text{ occurs}\\ 0, & \text{if } A \text{ does not occur.}\end{cases}$$

The quadratic $p_2(1-p_2)$ increases on the interval $[0,1/2]$, so $A(1-p_2,p_2)$ decreases on the same interval. Thus $A(\mathbf{p})$ is Schur-convex for $n=2$.

We have given two examples of a function in several variables with constant sum that attains its maximum or minimum value at the point where all the variables are equal. When you encounter such an inequality, you should suspect that a stronger version may be true. The function might also be Schur-convex or Schur-concave. For a superb account of the history, theory, and applications of majorization see Marshall and Olkin's definitive work [3].

REFERENCES

1. D. M. Bloom, A birthday problem, *Amer. Math. Monthly* 80 (1973), 1141–2.
2. William Feller, *An Introduction to Probability Theory and Its Applications*, Vol. 1, 3rd edition, John Wiley & Sons, New York, 1970.
3. Albert W. Marshall and Ingram Olkin, *Inequalities: Theory of Majorization and Its Applications*, Academic Press, New York, 1979.
4. Frederick Mosteller, *Fifty Challenging Problems in Probability with Solutions*, Addison-Wesley, Reading, MA, 1965.
5. A. G. Munford, A note on the uniformity assumption in the birthday problem, *The Amer. Statist.* 31 (1977), 119.
6. Philip F. Rust, The effect of leap years and seasonal trends on the birthday problem, *The Amer. Statist.* 30 (1976), 197–8.

Monte Carlo Simulation of Infinite Series

FREDERICK SOLOMON
Warren Wilson College
Swannanoa, NC 28778

Let c be a real number. A *Monte Carlo simulation* of c consists of these steps: First, a random experiment is devised and a random variable X is defined for the experiment such that the expectation of X satisfies $c=E(X)$. Second, the random experiment is performed a large number, K of times; let X_i denote the value of X on the ith experiment. By the Strong Law of Large Numbers,

$$c=E(X_i)=\lim_{K\to\infty}\frac{X_1+X_2+\cdots+X_K}{K}$$

with probability 1. Consequently, for large K, c "should be" approximately $(X_1+X_2+\cdots+X_K)/K$. This ratio is then the Monte Carlo estimate of c.

This method also covers the case in which the constant c is represented as the *probability of an event* A rather than directly as the expectation of a random variable. Namely if $c=P(A)$, then perform the random experiment through which event A is defined and define the random variable X by

$$X=\begin{cases}1, & \text{if } A \text{ occurs}\\ 0, & \text{if } A \text{ does not occur.}\end{cases}$$

Then $E(X) = P(A) = c$ and $X_1 + X_2 + \cdots + X_K$ is the total number of times A occurred on all K experiments.

The Buffon Needle Experiment is a classic method of simulating π using a Monte Carlo technique; it is a standard example in probability texts.

This paper presents several methods for Monte Carlo simulation of numbers that have infinite series representations. To simulate a number c, *each* of K simulations consists of generating values of random variables $U_1, U_2, \dots$ until some "stopping condition" is satisfied. Let N be the *maximum index* of the U_i generated. The random variable X is then set equal to some specific value depending on the values of N and $U_1, \dots, U_N$. For any such scheme to be feasible, the event $\{N = n\}$ must be a function of $U_1, \dots, U_n$, but *not* of any U_i for $i > n$. (This simply states that the question as to whether to stop after generating $U_1, \dots, U_n$ must be able to be determined on the basis of the U_i already generated. In probabilistic language N is called a *stopping time* [**1**, p. 259].)

Throughout the note $U_1, U_2, \dots$ will denote a sequence of independent, identically distributed random variables. We will be concerned only with the *order statistics* (that is, the relative ordering by magnitude of $U_1, U_2, \dots$); probabilities defined by the relative ordering of $U_1, U_2, \dots$ do not depend on the particular common distribution of U_i as long as it is *continuous*, in which case $P(U_i = U_j) = 0$ for $i \neq j$. However, for simplicity we will always assume that each U_i is *uniformly distributed on the unit interval* $[0, 1]$.

Any number can be simulated using an infinite series representation. For example, if $0 \leqslant c < 1$ has binary representation

$$c = \sum_{n=1}^{\infty} \frac{a_n}{2^n},$$

where $a_n = 0$ or 1 for each n, then c can be simulated in this way: The ith of K random experiments consists of generating U_1, U_2, ... independently, each uniformly distributed on $[0, 1]$, until $U_N < 1/2$. That is, $U_i \geqslant 1/2$ for $i = 1, \dots, N-1$. Then set $X_i = a_N$. Notice that

$$E(X) = \sum_{n=1}^{\infty} a_n \cdot P(N = n) = \sum_{n=1}^{\infty} a_n \cdot \frac{1}{2^n}.$$

Consequently the average of $X_1, \dots, X_k$ will be a Monte Carlo simulation of c. In this way I simulated these numbers:

c	Simulated Value	K
$3/4 = .11_2$	.7585	2000
$1/3 = .010101\dots_2$	.3360	1000

(This technique has one grave drawback: If one *already knows* the binary representation for c, then one hardly needs a Monte Carlo simulation to find it!)

The motivation for this paper, however, is more specific: How can constants such as π and e be simulated using a known series representation?

THEOREM I. *Let*

$$c = \sum_{n=2}^{\infty} \frac{a_n}{n!},$$

where integer a_n satisfies $0 \leqslant a_n \leqslant n-1$. Generate $U_1, U_2, \ldots$ until $U_N > U_{N-1}$. That is, $N \geqslant 2$ is the smallest index so that U_N exceeds its predecessor U_{N-1}. Define the random variable X in this way: If $a_N = 0$, then set $X = 0$. If $a_N > 0$ and if $U_N > U_{a_N}$, then set $X = 1$, otherwise set $X = 0$. Then $E(X) = c$.

Proof. There are $n!$ ways in which to order the n values $U_1, \ldots, U_n$, but there are only $n-1$ ways to order them in such a way that $\{N = n\}$ is satisfied. Consequently

$$\begin{aligned} P(N=n) &= P(U_1 > U_2 > \cdots > U_{n-1}, \text{but } U_n > U_{n-1}) \\ &= (n-1)/n! \end{aligned}$$

If $a_n > 0$, then among the $n-1$ orderings of $U_1, \ldots, U_n$ that satisfy the event $\{N = n\}$, there are a_n such that $U_n > U_{a_n}$. Thus

$$P(X=1 | N=n) = P\big(U_n > U_{a_n} | N=n\big) = a_n/(n-1).$$

Note that if $a_n = 0$, then $P(X = 1 | N = n) = 0 = a_n/(n-1)$ also. Since the range of X is $\{0, 1\}$,

$$\begin{aligned} E(X) &= 1 \cdot P(X=1) + 0 \cdot P(X=0) \\ &= \sum_{n=2}^{\infty} P\big(U_n > U_{a_n} | N=n\big) \cdot P(N=n) \\ &= \sum_{n=2}^{\infty} \frac{a_n}{n!}. \end{aligned}$$

Example 1. Theorem I can be used to simulate

$$e - 2 = \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \cdots.$$

Since $a_n = 1$ for $i = 2, 3, \ldots$, the ith random experiment in the set of K consists of these steps.

Step 1. Generate $U_1, U_2, \ldots$ until $U_N > U_{N-1}$.

Step 2. If $U_N > U_1$, then set $X_i = 1$; otherwise set $X_i = 0$.

A computer simulation with $K = 10{,}000$ random experiments resulted in a simulated value of .7130 (compared with the actual value of .71828). The table at the end of this paper shows "how good" this simulation is.

Theorem I applied to Example 1 implies that in an indefinitely long sequence $U_1, U_2, \ldots$ of random variables, $e - 2 = P$ (the first U_N to exceed its predecessor also exceeds U_1). This fact is used in von Neumann's method for generating exponentially distributed random variables [3, p. 452–455].

Example 2. Consider the series

$$\begin{aligned} \frac{1}{2e} &= \frac{1}{2} \cdot \left(\frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \cdots\right) \\ &= \frac{1}{3!} + \frac{2}{5!} + \frac{3}{7!} + \cdots. \end{aligned}$$

Theorem I yields the following algorithm for simulating $1/2e$. The ith random experiment consists of:

Step 1. Generate $U_1, U_2, \ldots$ until $U_N > U_{N-1}$.

Step 2. If N is odd and if $U_N > U_{(N-1)/2}$, then set $X_i = 1$; otherwise set $X_i = 0$.

A simulation of $K=10{,}000$ random experiments resulted in a simulated value of $1/2e$ of .1825 compared with the actual value of .18394.

THEOREM II. *Let*

$$c=\frac{1}{k_1}-\frac{1}{k_2}+\frac{1}{k_3}-\frac{1}{k_4}+\cdots,$$

where integers $k_1, k_2, \ldots$ *satisfy* $1 \leqslant k_1 < k_2 < \cdots$. *Generate* $U_1, U_2, \ldots$ *until* $U_N > U_1$. *That is,* $N \geqslant 2$ *is the smallest index so that* U_N *exceeds the* first *number generated,* U_1. *Define the random variable* X *in this way: Find the smallest odd integer* $2j-1$ (*for* $j \geqslant 1$) *so that*

$$k_{2j-1} < N.$$

If no such j *exists, set* $X=0$. *If* j *exists, and* $N \leqslant k_{2j}$, *then set* $X=1$, *otherwise set* $X=0$. *Then* $E(X)=c$.

Proof. For positive integers $0<r<s$

$$\begin{aligned} &P(U_1>U_2,\ldots,U_1>U_r, \text{ but } U_t>U_1 \text{ for some } r<t\leqslant s)\\ &\quad = P(U_1>U_2,\ldots,U_1>U_r) - P(U_1>U_2,\ldots,U_1>U_s)\\ &\quad = \frac{1}{r}-\frac{1}{s}. \end{aligned}$$

Therefore, the definition of N in the statement of Theorem II implies that

$$\begin{aligned} E(X) &= P(X=1)\\ &= \sum_{j=1}^{\infty} P\big(k_{2j-1}<N\leqslant k_{2j}\big)\\ &= \sum_{j=1}^{\infty} P\big(U_1>U_2,\ldots,U_1>U_{k_{2j-1}}, \text{ but } U_t>U_1\\ &\qquad\qquad \text{for some } k_{2j-1}<t\leqslant k_{2j}\big)\\ &= \sum_{j=1}^{\infty}\left(\frac{1}{k_{2j-1}}-\frac{1}{k_{2j}}\right). \end{aligned}$$

Example 3.

$$\frac{\pi}{4}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots.$$

For $j=1,2,\ldots$ set $k_{2j-1}=4j-3$ and $k_{2j}=4j-1$. Then the notation agrees with that of Theorem II; this algorithm will generate for the ith value the random variable X_i whose expectation is $\pi/4$:

Step 1. Generate $U_1, U_2, \ldots$ until $U_N > U_1$.

Step 2. Find the largest $j \geqslant 1$ so that $4j-3<N$. (Note that such a j always exists since $N \geqslant 2$.) If $N \leqslant 4j-1$, then set $X=1$, otherwise set $X=0$.

With $K=10{,}000$ random experiments, the simulated value of $\pi/4$ was .7890 compared with the actual value .7854.

Example 4.

$$e^{-1} = \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \cdots.$$

Set $k_{2j-1} = (2j)!$ and $k_{2j} = (2j+1)!$ for $j = 1, 2, \ldots$. To generate X_i use the same Step 1 as in Example 3; Step 2 becomes:

Step 2. Find the largest j so that $(2j)! < N$. If $N \leqslant (2j+1)!$, then set $X_i = 1$; otherwise set $X_i = 0$. (If in fact $N = 2$, then there exists no j so that $(2j)! < N$ in which case set $X_i = 0$.)

Example 5. For integer $s \geqslant 1$

$$\ln\left(1 + \frac{1}{s}\right) = \frac{1}{s} - \frac{1}{2s^2} + \frac{1}{3s^3} - \frac{1}{4s^4} + \cdots.$$

Set $k_{2j-1} = (2j-1)s^{2j-1}$ and $k_{2j} = 2js^{2j}$ for $j = 1, 2, \ldots$. After generating $U_1, U_2, \ldots$ as in Step 1 of Example 3, Step 2 becomes:

Step 2. Find the largest integer j such that $(2j-1)s^{2j-1} < N$. If such a j does not exist, then set $X_i = 0$. If such a j exists and $N \leqslant 2js^{2j}$, then set $X_i = 1$; otherwise set $X_i = 0$.

Note how Step 2 simplifies when simulating $\ln(2)$ for which $s = 1$: If N is even, then set $X_i = 1$; otherwise set $X_i = 0$.

Note that the natural logarithm of any positive integer can be simulated using this example and the following decomposition:

$$\begin{aligned}\ln(j) &= (\ln(j) - \ln(j-1)) + (\ln(j-1) - \ln(j-2)) \\ &\quad + \cdots + (\ln(2) - \ln(1)) \\ &= \ln\left(1 + \frac{1}{j-1}\right) + \ln\left(1 + \frac{1}{j-2}\right) + \cdots + \ln\left(1 + \frac{1}{1}\right).\end{aligned}$$

And then the natural logarithm of any positive rational can be simulated as the difference of the simulated values of the logarithms of integers.

In order to phrase Theorem III below, a technical lemma is required. Since our interest is in deriving algorithms, we phrase the lemma as

Algorithm A. Let r and s be integers with $0 \leqslant r \leqslant s!$ Let $V_1, \ldots, V_s$ be continuous, independent, and identically distributed random variables. This algorithm articulates a method for defining an event A in terms of the order statistics of $V_1, \ldots, V_s$ so that A can happen in r ways. Thus $P(A) = r/s!$ The algorithm proceeds recursively:

i) If $s = 0$ or 1, the algorithm is obvious: Namely, set $A = \varnothing$ if $s = 0$ or if $s = 1$ and $r = 0$. If $s = 1$ and $r = 1$, then set $A =$ sure event (i.e., $P(A) = 1$).

ii) If $s = 2$, set $A = \varnothing$ if $r = 0$ and set $A =$ sure event if $r = 2$. If $r = 1$, set $A =$ the event $\{V_1 < V_2\}$.

iii) Assume that $A = A_{r,s}$ has been defined for all r and s satisfying $0 \leqslant r \leqslant s!$ and $s < s_0$. Now assume that $s = s_0$.

Step a. If $r = 0$, then set $A = \varnothing$. If $r = s_0!$, set $A =$ sure event.

Step b. Assume that $0 < r < s_0!$ Find the unique integer p satisfying

$$1 \leqslant p \leqslant s_0 - 1$$
$$p! \leqslant r < (p+1)!$$

Such a p exists since $0 < r < s_0!$

Step c. Given this value of p, find the unique integer q satisfying

$$1 \leqslant q \leqslant p$$
$$q \cdot p! \leqslant r < (q+1) \cdot p!$$

Step d. Define the event

$$B_0 = \left\{ \max(V_1, \dots, V_p) < V_{p+1} < \cdots < V_{s_0} \right\}.$$

B_0 can happen in $p!$ ways. ($p!$ = number of ways to order $V_1, \dots, V_p$.) By exchanging V_t for $t = 1, \dots, p$ with V_{s_0} successively we can define p events:

$$B_t = \left\{ \max(V_1, \dots, V_{t-1}, V_{s_0}, V_{t+1}, \dots, V_p) \right.$$
$$\left. < V_{p+1} < \cdots < V_{s_0 - 1} < V_t \right\}$$

for $t = 1, \dots, p$. Note that $B_0, B_1, \dots, B_p$ are pairwise disjoint and each has $p!$ ways of occurring ($p!$ ways to order the p random variables in the maximum). Given p and q from Steps b and c, set

$$B = B_1 \cup \cdots \cup B_q.$$

Then B can happen in $q \cdot p!$ ways.

Step e. Set $d = r - q \cdot p!$ Thus $0 \leqslant d < (q+1) \cdot p! - q \cdot p! = p!$. But $p < s_0$. Consequently, by the inductive hypothesis, an event C_d determined by the order statistics of $V_1, \dots, V_p$ can be defined, which can occur in d ways. Thus

$$C = \left\{ (V_1, \dots, V_p) \in C_d \text{ and } \max(V_1, \dots, V_p) < V_{p+1} < \cdots < V_s \right\}$$
$$\subseteq B_0$$

and C can happen in d ways. Since B_0 is disjoint from B,

$$A = C \cup B = C \cup B_1 \cup \cdots \cup B_q$$

can happen in $d + q \cdot p! = r$ ways. This completes the steps (and proof) of Algorithm A.

THEOREM III. *Let*

$$c = \sum_{n=2}^{\infty} \frac{a_n}{n!},$$

where integer a_n *satisfies* $0 \leqslant a_n \leqslant (n-2)!$. *Generate* $U_1, U_2, \dots$ *until* $U_N > U_1$. *Suppose that* A_N *is an event defined in terms of the* $N-2$ *random variables* $U_2, \dots, U_{N-1}$ *so that* A_N *can happen in* a_N *ways.* (*Algorithm A shows how this can be done.*) *Define the random variable* X *in this way: If* $U_2, \dots, U_{N-1}$ *satisfies event* A_N, *then set* $X = 1$; *otherwise set* $X = 0$. *Then* $E(X) = c$.

Proof. Given the event

$$\{N = n\} = \{U_1 > U_2, \dots, U_1 > U_{n-1}, \text{ but } U_n > U_1\}$$

the random variables $U_2, \dots, U_{n-1}$ are independent and identically distributed (although their common distribution is not the original distribution). Thus

$$P(U_2, \dots, U_{n-1} \text{ satisfies event } A_n | N = n) = \frac{a_n}{(n-2)!}.$$

Consequently

$$\begin{aligned} E(X) &= P(X=1) \\ &= \sum_{n=2}^{\infty} P(U_2,\dots,U_{n-1} \text{ satisfies } A_n | N=n)\cdot P(N=n) \\ &= \sum_{n=2}^{\infty} \frac{a_n}{(n-2)!}\frac{1}{n(n-1)}. \end{aligned}$$

The last equality holds since there are $n!$ ways to order $U_1,\dots,U_n$ of which $(n-2)!$ satisfy the additional property that U_n is the largest and U_1 the second largest (i.e., satisfies $\{N=n\}$).

Example 6. (See [2] for the following and many other series to which the results in this paper are applicable.)

$$\frac{\pi}{8} - \frac{\ln(2)}{2} = \frac{1}{2\cdot 3\cdot 4} + \frac{1}{6\cdot 7\cdot 8} + \frac{1}{10\cdot 11\cdot 12} + \cdots.$$

Note that $a_n = 0$ if n is not a multiple of 4 while $a_n = (n-3)!$ if a_n is a multiple of 4. Theorem III yields the following algorithm to generate X_i so that $E(X_i) = \pi/8 - \ln(2)/2$:

Step 1. Generate $U_1, U_2, \dots$ until $U_N > U_1$.

Step 2. If N *is not* a multiple of 4, then $a_N = 0$; in this case set $X_i = 0$ and the simulation is complete. If N *is* a multiple of 4, proceed to Step 3 to find the value of X_i.

Step 3. $a_N = (N-3)!$. Since $1\cdot(N-3)! = a_N < 2\cdot(N-3)!$, Steps b and c of Algorithm A imply that

$$p = N-3 \quad\text{and}\quad q = 1.$$

In applying Algorithm A, we set $V_1 = U_2$, $V_2 = U_3,\dots,V_{N-2} = U_{N-1}$. Since $d=0$ and $q=1$,

$$\begin{aligned} A = A_N = B_1 &= \{\max(V_{N-2}, V_2, V_3,\dots,V_{N-3}) < V_1\} \\ &= \{\max(U_{N-1}, U_3, U_4,\dots,U_{N-2}) < U_2\}. \end{aligned}$$

In summary, set $X=1$ if N is a multiple of 4 and U_2 is the largest among $U_2, U_3,\dots,U_{N-1}$. (The actual value of $c = \pi/8 - \ln(2)/2$ is .04613; the simulated value was .04667 on $K = 10{,}000$ experiments.)

Example 7. This example illustrates an application of Algorithm A in the case in which $d \neq 0$. Consider the series

$$c = \sum_{n=4}^{\infty} \frac{(n-3)!+1}{n!}$$

using Theorem III. Then $a_n = (n-3)! + 1$ for $n \geqslant 4$. We need to find an event A_n defined in terms of the order statistics of $U_2,\dots,U_{n-1}$ that can happen in a_n ways. In the notation of Algorithm A, $V_1 = U_2$, $V_2 = U_3,\dots,V_{n-2} = U_{n-1}$; $s = n-2$ and $r = a_n = (n-3)! + 1$. Steps b and c require

$$p = n-3, \quad\text{and}\quad q = 1$$

and Step e requires

$$d = 1.$$

The reader can verify that the events B_1 and C of Steps d and e are

$$\begin{aligned} B_1 &= \{\max(V_{n-2}, V_2, V_3, \dots, V_{n-3}) < V_1\} \\ &= \{\max(U_{n-1}, U_3, U_4, \dots, U_{n-2}) < U_2\}, \\ C &= \{V_1 < V_2 < \cdots < V_{n-2}\} \\ &= \{U_2 < U_3 < \cdots < U_{n-1}\}. \end{aligned}$$

The event $A = B_1 \cup C$ can happen in $r = (n-3)! + 1$ ways. In summary, the simulation of X_i consists of these steps:

Step 1. Generate $U_1, U_2, \dots$ until $U_N > U_1$.

Step 2. If $N = 2$ or 3, then set $X_i = 0$. If $N \geqslant 4$ and (with $n = N$) $U_2, \dots, U_{n-1}$ satisfies $A = B_1 \cup C$, then set $X_i = 1$; otherwise set $X_i = 0$.

Numerous other algorithms can be developed based on such stopping times as N = second index for which U_N exceeds U_1 or N = smallest index so that U_N is larger than exactly three of $U_1, \dots, U_{N-1}$ or $N = \cdots$ Each of these definitions leads to a formula for a probability in terms of an infinite series and consequently a method for simulating that probability. One of these stopping times leads to an important example and is a special case of the following.

THEOREM IV. *Let*

$$c = \sum_{n=2}^{\infty} \frac{a_n}{n!} t^n$$

where integer a_n satisfies $0 \leqslant a_n \leqslant (n-2)!$ and $0 \leqslant t \leqslant 1$. Generate $U_1, U_2, \dots$ until $U_N > U_1$ or $U_N < 1 - t$, whichever occurs first. If $U_N < 1 - t$, then set $X = 0$. If $U_N > 1 - t$, then use Algorithm A to find an event A_{N-2} that can happen in a_N ways. If $U_2, \dots, U_{N-1}$ satisfies A_{N-2}, then set $X = 1$; otherwise set $X = 0$. Then $E(X) = c$.

The proof is left to the reader.

Example 7. Fix t with $0 \leqslant t \leqslant 1$.

$$e^t - (1 + t) = \frac{t^2}{2!} + \frac{t^3}{3!} + \cdots.$$

To simulate $e^t - (1+t)$ and thereby simulate e^t, each experiment generates X in this way: Generate $U_1, U_2, \dots$ until $U_N > U_1$ or $U_N < 1 - t$. If $U_1 > U_2 > \cdots > U_{N-1} > 1 - t$ and $U_N > U_1$, then set $X = 1$; otherwise set $X = 0$. (This is equivalent to, but not quite the same as the method prescribed using Algorithm A.)

How many individual random experiments are required to simulate an accurate estimate of c? $X_1, \dots, X_K$ are independent, identically distributed where $X_i = 1, 0$ with respective probabilities $c, 1 - c$. Thus

$$E(X_i) = c, \qquad \mathrm{Var}(X_i) = \text{Variance of } X_i = c(1 - c),$$

where $0 \leqslant c \leqslant 1$ is the number to be simulated. Thus the sum $S_K = X_1 + \cdots + X_K$ has

$$\begin{aligned} E(S_K) &= Kc, \\ \mathrm{Var}(S_K) &= Kc(1-c). \end{aligned}$$

By Chebyshev's Inequality

$$P\left(\left|\frac{S_K}{K}-c\right|<\varepsilon\right)=P(|S_K-Kc|<K\varepsilon)$$
$$\geqslant 1-\frac{Kc(1-c)}{K^2\varepsilon^2}$$
$$\geqslant 1-\frac{1}{4K\varepsilon^2},$$

since $0\leqslant c\leqslant 1$ implies that $0\leqslant c(1-c)\leqslant 1/4$. Thus to be α sure that S_K/K is within ε of c, set

$$\alpha\leqslant 1-\frac{1}{4K\varepsilon^2},$$

or

$$K\geqslant\frac{1}{4(1-\alpha)\varepsilon^2}.$$

For example, to be 90% sure ($\alpha=.9$) that the simulated value of c will be within .01 ($\varepsilon=.01$) of c, the number of experiments K required is 25,000. (Using the Central Limit Theorem rather than Chebyshev's Inequality yields an estimate for K that is the same order of magnitude.) A lot of experiments!

We conclude with an analysis of "how good" the simulations in the examples actually are. The Central Limit Theorem implies

$$P\left(\left|\frac{S_K}{K}-c\right|>\varepsilon\right)=P\left(\left|\frac{|S_K-Kc|}{\sqrt{Kc(1-c)}}>\frac{\sqrt{K}\,\varepsilon}{\sqrt{c(1-c)}}\right|\right)$$
$$\cong 2\left(1-\Phi\left(\sqrt{K}\,\varepsilon/\sqrt{c(1-c)}\right)\right)$$

where Φ is the normal distribution function, mean 0, variance 1. The following table summarizes the simulations in the examples. The last column is the probability that with K simulations, the simulated value of c would be further from the actual value than was the case with our simulations. ($\varepsilon=$ |actual value−simulated value|).

Example	Value to be Simulated	Actual Value	Simulated *Value*	K	$2\left(1-\Phi\left(\frac{\sqrt{K}\varepsilon}{\sqrt{c(1-c)}}\right)\right)$
1	$e-2$	.71828	.7130	10,000	.24
2	$1/2e$	.18394	.1825	10,000	.71
3	$\pi/4$	.78540	.7890	10,000	.26
5	$\ln(2)$	.69315	.6740	2,000	.06
6	$\frac{\pi}{8}-\frac{\ln(2)}{2}$	.046125	.04667	10,000	.83

I would like to thank the referees for their suggestions substantially improving the quality of exposition.

REFERENCES

1. K. L. Chung, *A Course in Probability Theory*, 2nd edition, Academic Press, New York, 1974.
2. L. B. W. Jolley, *Summation of Series*, 2nd edition, Dover, New York, 1961.
3. S. M. Ross, *Introduction to Probability Models*, 3rd edition, Academic Press, New York, 1985.

PROBLEMS

LOREN C. LARSON, *editor*
St. Olaf College

GEORGE GILBERT, *associate editor*
Texas Christian University

Proposals

To be considered for publication, solutions should be received by November 1, 1991.

1373. *Proposed by William P. Wardlaw, U.S. Naval Academy, Annapolis, Maryland.*

Find the set S' of all accumulation points of the set $S = \{\varphi(n)/n\colon n \in \mathbf{N}\}$, where φ is the Euler phi function and $\mathbf{N}$ is the set of positive integers.

1374. *Proposed by David Moews and Michael Reid, students, University of California, Berkeley, California.*

Let H be a unit n-dimensional hypercube, and A be any set of hyperfaces of H. Let H_A be the figure created by adjoining unit hypercubes at each hyperface in A. Show that, regardless of A, H_A tessellates n-space.

1375. *Proposed by Lorraine L. Foster, California State University, Northridge, California.*

Prove that for each integer $k \geq 3$ there exist positive integers $n_1, n_2, \ldots, n_k$ such that $\Pi_{i \neq j} n_i \equiv 1 \pmod{n_j}$, for $j = 1, 2, \ldots, k$. (Note: Problem **1339**, February 1990; Solution, February 1991, treats the case $k = 3$.)

1376. *Proposed by Eric Canning, student, and Marion B. Smith, California State University, Bakersfield, California.*

If p is a prime and n an integer such that $1 < n \leq p$, then $\varphi(\Sigma_{k=0}^{p-1} n^k) \equiv 0 \pmod{p}$, where φ is the Euler phi function.

1377. *Proposed by Hüseyin Demir, Middle East Technical University, Ankara, Turkey.*

Let DEF be a variable triangle inscribed in triangle ABC, and let U, X, V, Y, W, Z be the midpoints of the line segments BD, DC, CE, EA, AF, and FB, respectively.

ASSISTANT EDITORS: CLIFTON CORZATT, BRUCE HANSON, RICHARD KLEBER, KAY SMITH *and* THEODORE VESSEY, *St. Olaf College and* MARK KRUSEMEYER, *Carleton College. We invite readers to submit problems believed to be new and appealing to students and teachers of advanced undergraduate mathematics. Proposals should be accompanied by solutions, if at all possible, and by any other information that will assist the editors and referees. A problem submitted as a Quickie should have an unexpected, succinct solution. An asterisk (*) next to a problem number indicates that neither the proposer nor the editors supplied a solution.*

Solutions should be written in a style appropriate for Mathematics Magazine. Each solution should begin on a separate sheet containing the solver's name and full address.

Solutions and new proposals should be mailed in duplicate to Loren C. Larson, Department of Mathematics, St. Olaf College, Northfield, MN 55057.

Show that the expression

$$|UVW| + |XYZ| - \tfrac{1}{2}|DEF|$$

for areas is constant.

Quickies

Answers to the Quickies are on page 206.

Q778. *Proposed by Ken Rebman, California State University, Hayward, California.*
Find the area between the circumscribed and inscribed circles of the regular 37-gon with sides of length 1.

Q779. *Proposed by Murray S. Klamkin, University of Alberta, Edmonton, Alberta, Canada.*
Determine the best upper and lower bounds for the sum

$$\frac{a}{f+a+b} + \frac{b}{a+b+c} + \frac{c}{b+c+d} + \frac{d}{c+d+e} + \frac{e}{d+e+f} + \frac{f}{e+f+a}$$

where a, b, c, d, e, and f are nonnegative and no denominator is zero.

Q780. *Proposed by Norman Schaumberger, Hofstra University, Hempstead, New York.*
If a, b, and c are positive, then

$$\left(\frac{a}{b}\right)^{a/b}\left(\frac{b}{c}\right)^{b/c}\left(\frac{c}{a}\right)^{c/a} \geq 1 \geq \left(\frac{a}{b}\right)^{b/a}\left(\frac{b}{c}\right)^{c/b}\left(\frac{c}{a}\right)^{a/c}.$$

Solutions

Closure of Rational Functions **June 1990**

1348. *Proposed by David Callan, University of Bridgeport, Bridgeport, Connecticut.*
A *Monthly* problem (E 3194, Feb. 1987; Solution March 1989) reads: "Let S be the smallest set of rational functions containing x and y, and closed under subtraction and reciprocals (of nonzero functions). Show that $1 \notin S$." Characterize those rational functions that are in S.

Solution by Mordechai Falkowitz, Tel Aviv, Israel.
We will assume that all polynomials have rational coefficients. Denote the set of those polynomials in x and y, all of whose terms have even (total) degree, by P, and the analogous set for odd degree terms by Q. *Claim*: The set S equals the set T of all rational functions of the form p/q or q/p, with $p \in P, q \in Q$, and nonzero denominators. (Note that $Q \subseteq T$, while $P \cap T = \{0\}$.)

To prove the claim, first note that T is clearly closed under taking reciprocals of nonzero functions, and that it is straightforward to show T is closed under subtraction. Therefore, $S \subseteq T$. To show $T \subseteq S$, we use the following lemma.

LEMMA. (i) *S is a vector space over the rationals.* (ii) *S is closed under taking products with an odd number of factors.*

Proof. (i) If $f, g \in S$, then $0 = g - g \in S, -g = 0 - g \in S$, and so $f + g = f - (-g) \in S$. If $f \in S$, $f \neq 0$, then for any positive integer $n, n/f = 1/f + \cdots + 1/f \in S$, so $f/n \in S$. Thus, for any positive rational number $m/n, (m/n)f = f/n + \cdots + f/n \in S$ and $-(m/n)f \in S$.

(ii) Clearly, it is enough to show this for products of three nonzero factors $f, g, h \in S$. First consider the special case $h = g$. If also $g = 1/f$, then $fgh = g \in S$; otherwise, using (i), $fgh = fg^2 = ((g - 1/f)^{-1} - 1/g)^{-1} + g \in S$. For the general case, note that $g + h \in S$ and therefore, using (i) and the special case, $fgh = (1/2)f(g+h)^2 - (1/2)fg^2 - (1/2)fh^2 \in S$.

It is immediate from the lemma that $Q \subseteq S$. If $q \in Q, q \neq 0$, then applying (ii) to $1/q$ along with an even number of factors x and y shows that for any monomial m of even degree, $m/q \in S$. Hence by (i), $p/q \in S$ for every $p \in P$. Now take reciprocals to complete the proof that $T \subseteq S$.

Also solved by S. F. Barger, Con Amore Problem Group (Denmark), and the proposer. There was one slightly, but significantly, incorrect solution, and one alternate definition of S that, however, did not characterize which rational functions are in S.

Fields and Invertible Matrices **June 1990**

1349. *Proposed by William P. Wardlaw, U.S. Naval Academy, Annapolis, Maryland.*

Let K be a field, n a positive integer, and $\mathbf{I}$ the $n \times n$ identity matrix. Give necessary and sufficient conditions on n and K such that for every $n \times n$ matrix $\mathbf{A}$ over K there is an element a in K such that $\mathbf{A} + a\mathbf{I}$ is invertible.

Solution by Athanasiadis Christos, student, Massachusetts Institute of Technology, Cambridge, Massachusetts.

Let k be the cardinal number of K. We show that a necessary and sufficient condition is that $k > n$.

Suppose $k > n$ and let $\mathbf{A}$ be an $n \times n$ matrix over K. Then $\det(\mathbf{A} + x\mathbf{I})$ is a monic polynomial in x of degree n. Hence it cannot have more than n zeros in K, so there is an element a of K such that $\det(\mathbf{A} + a\mathbf{I})$ is different from zero, and hence, $\mathbf{A} + a\mathbf{I}$ is invertible.

Suppose $k \leqslant n$ and let $a_1, a_2, \ldots, a_k$ be the distinct elements of K. Let $\mathbf{A} = \operatorname{diag}(a_1, a_2, \ldots, a_k, 0, \ldots, 0)$. Then for all a in K, $\det(\mathbf{A} + a\mathbf{I}) = (a_1 + a)(a_2 + a) \cdots (a_k + a)a^{n-k}$. Since $-a$ is one of the elements a_j, $\det(\mathbf{A} + a\mathbf{I}) = 0$ and this completes the proof.

Also solved by S. F. Barger, Duane Broline, David Callan, Con Amore Problem Group (Denmark), F. J. Flanigan, Heather Levi, N. J. Lord (England), John D. O'Neill, Stephen G. Penrice, Ioan Sadoveanu, Gary K. Schwartz, and the proposer.

Variation on the Tower of Hanoi **June 1990**

1350. *Proposed by Hugh Noland, Chico, California.*

In the well-known Tower of Hanoi puzzle one starts with three pegs, two of which are empty and one of which contains n disks, no two of the same size, stacked in order of size, with the smallest on top. It is required to move all the disks to one of the empty pegs, by moving one disk at a time, subject to the condition that no disk ever rests on a smaller one. It is easy to show that the number of moves required is $2^n - 1$.

Suppose instead that one has $2n$ disks, numbered according to size, with the smallest numbered 1. If all the odd-numbered disks occupy one peg and all the even-numbered disks another, stacked according to size, how many moves are required to move all the disks onto the empty peg, the requirement again being that no disk ever rests on a smaller?

I. *Solution by Norman F. Lindquist, Western Washington University, Bellingham, Washington.*

Let T_n represent the least number of moves necessary to move the $2n$ disks to the empty peg. We will show

$$T_n = T_{n-3} + (45)4^{n-3}, \qquad n \geqslant 3$$

with $T_0 = 0$, $T_1 = 2$, and $T_2 = 11$.

From this, it is easy to show by induction that

$$T_{3k} = \tfrac{5}{7}4^{3k} - \tfrac{5}{7}, \qquad T_{3k+1} = \tfrac{5}{7}4^{3k+1} - \tfrac{6}{7}, \qquad T_{3k+2} = \tfrac{5}{7}4^{3k+2} - \tfrac{3}{7},$$

which is put more succinctly in the formula,

$$T_n = \left\lfloor \tfrac{5}{7}4^n \right\rfloor.$$

To see this, name the peg with the odd-numbered disks A, the peg with the even-numbered disks B, and the empty peg C. Let H_n represent the number of moves required to move n disks in the Tower of Hanoi puzzle. We identify four key moves.

1. *Move disk $2n$ from peg B to peg C.* When this move is accomplished, we may finish by moving the $2n-1$ disks on peg A to peg C. The number of moves required for both operations is $1 + H_{2n-1} = 2^{2n-1}$ moves.

2. *Move disk $2n-2$ from peg B to peg A.* To accomplish this, peg A must have only disk $2n-1$ and the other disks are stacked in order on peg C. Moving the $2n-3$ disks from peg C onto peg A will allow us to do the first key move. The number of moves required to do both operations is $1 + H_{2n-3} = 2^{2n-3}$ moves.

3. *Move disk $2n-3$ from peg A to peg C.* To do this we assume that peg C is empty and that all of the disks except $2n-1$ and $2n-3$ are on peg B. After this move, we move the top $2n-4$ disks from peg B onto peg C on top of disk $2n-3$, setting the stage for the second key move. The number of moves required for both operations is $1 + H_{2n-4} = 2^{2n-4}$ moves.

4. *Move disk $2n-5$ from peg A to peg B.* To do this, disks 1 to $2n-6$ must be on peg C. After this move, we move the $2n-6$ disks from peg C onto disk $2n-5$ on peg B, which will allow us to do the third key move. The number of moves required to do these two operations is $1 + H_{2n-6} = 2^{2n-6}$.

The number of moves required to be in position to do the last key move (where we have three disks on peg A, three disks on peg B and the rest of the disks, in order from 1 to $2n-6$, on peg C) is just T_{n-3}. Consolidating this information gives

$$\begin{aligned} T_n &= 2^{2n-1} + 2^{2n-3} + 2^{2n-4} + 2^{2n-6} + T_{n-3} \\ &= T_{n-3} + (1+2^2)(1+2^3)4^{n-3} = T_{n-3} + (45)4^{n-3}. \end{aligned}$$

We let $T_0 = 0$ and it is easy to see that $T_1 = 2$. With $n = 2$, moving disk 1 from peg A to C allows us to use the second and first key moves. Thus, $T_2 = 1 + (1 + H_1) + (1 + H_3) = 11$. This completes the proof.

II. *Solution by David G. Poole, Trent University, Peterborough, Ontario, Canada.*

Label the pegs A, B, and C and without loss of generality assume that the odd-numbered disks are initially on A, the even-numbered disks on B, stacked according to size. Let A_n, B_n, and C_n be the minimum number of moves required to move all $2n$ disks to A, B, and C, respectively. We will determine all three functions.

Set $\mathbf{X}_n = (A_n, B_n, C_n)$. Then clearly, $\mathbf{X}_0 = (0,0,0)$, $\mathbf{X}_1 = (3,1,2)$ and we have the following recurrences: $A_n = B_{n-1} + 1 + (2^{2n-2} - 1) + 1 + (2^{2n-1} - 1)$ [move the first $2n-2$ disks into position on top of disk $2n$ on peg B, move disk $2n-1$ to C, move the top $2n-2$ disks from B to C, move disk $2n$ from B to A, then move all $2n-1$ disks from C to A]. Simplified, this gives $A_n = B_{n-1} + 3 \cdot 4^{n-1}$. In a similar way we find $B_n = C_{n-1} + 1 + (2^{2n-2} - 1) = C_{n-1} + 4^{n-1}$ [move $2n-2$ disks into position on C, move disk $2n-1$, to B, then move the $2n-2$ disks from C to B]; and $C_n = A_{n-1} + 1 + (2^{2n-1} - 1) = A_{n-1} + 2 \cdot 4^{n-1}$ [move the first $2n-2$ disks into position on top of disk $2n-1$ on A, move disk $2n$ to C, then move all $2n-1$ disks from A to C].

We can write these recurrences in matrix form as

$$\mathbf{X}_n = \mathbf{X}_{n-1}\mathbf{P} + \mathbf{X}_1 4^{n-1}, \qquad n \geqslant 1,$$

where

$$\mathbf{P} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Unfolding the recurrence, we obtain

$$\mathbf{X}_n = \mathbf{X}_0\mathbf{P}^n + \mathbf{X}_1\left(\sum_{k=0}^{n-1} 4^k \mathbf{P}^{n-k-1}\right) = \mathbf{X}_1\left(\sum_{k=0}^{n-1} 4^k \mathbf{P}^{n-k-1}\right) = \mathbf{X}_1(\mathbf{P} - 4\mathbf{I})^{-1}(\mathbf{P}^n - 4^n\mathbf{I}),$$

where $\mathbf{I}$ denotes the 3×3 identity matrix and the last equality follows from the facts that (a) $4\mathbf{I}$ is a scalar matrix and hence commutes with all 3×3 matrices, in particular $\mathbf{P}$, and (b) $\mathbf{P}$ is a permutation matrix, so cannot have 4 as an eigenvalue, and therefore $\mathbf{P} - 4\mathbf{I}$ is invertible.

Now

$$\mathbf{X}_1(\mathbf{P} - 4\mathbf{I})^{-1} = -\frac{1}{63}(54, 27, 45) = -\frac{1}{7}(6, 3, 5)$$

and

$$\mathbf{P}^n - 4^n\mathbf{I} = \begin{cases} \begin{pmatrix} 1-4^n & 0 & 0 \\ 0 & 1-4^n & 0 \\ 0 & 0 & 1-4^n \end{pmatrix}, & \text{if } n \equiv 0 \pmod 3, \\ \begin{pmatrix} -4^n & 1 & 0 \\ 0 & -4^n & 1 \\ 1 & 0 & -4^n \end{pmatrix}, & \text{if } n \equiv 1 \pmod 3, \\ \begin{pmatrix} -4^n & 0 & 1 \\ 1 & -4^n & 0 \\ 0 & 1 & -4^n \end{pmatrix}, & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Multiplying, we obtain

$$\mathbf{X}_n = \begin{cases} \frac{1}{7}(6(4^n - 1), 3(4^n - 1), 5(4^n - 1)), & \text{if } n \equiv 0 \pmod 3, \\ \frac{1}{7}(6(4^n) - 3, 3(4^n) - 5, 5(4^n) - 6), & \text{if } n \equiv 1 \pmod 3, \\ \frac{1}{7}(6(4^n) - 5, 3(4^n) - 6, 5(4^n) - 3), & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

The third components contain the solution to the problem as posed.

III. *Solution by Allen J. Schwenk, Western Michigan University, Kalamazoo, Michigan.*

For $2n$ disks with $2n \equiv r \pmod 3$, where $0 \leqslant r \leqslant 2$, we shall show that the minimum number of moves is $\frac{5}{7}(2^{2n} - 2^r) + r$, but let us solve the more general question:

Given any starting pattern of N stacked disks (with no disk resting on a smaller one), what is the minimum number of moves needed to stack all the disks onto one peg?

We label the pegs A, B, and C and identify the starting position by defining a position function $p(i)$ to be the name of the peg at which i is originally stacked. The posed question has

$$p(i) = \begin{cases} A & \text{if } i \text{ is odd,} \\ B & \text{if } i \text{ is even.} \end{cases}$$

We also define a destination function $d(i)$ as the name of the peg where the first i disks must be stacked in order to allow the movement of disk $i+1$ as needed. That is, we define $d(i)$ sequentially starting with $d(N)$ assigned the label of the destination. Next, if it happens that $p(N) = d(N)$, it is not necessary to move disk N at all, and so we also assign $d(N\text{-}1) = d(N)$. Otherwise, we need to move disk N from $p(N)$ to $d(N)$. To permit this, the other disks must be stacked on the third disk. Consequently, we define $d(N-1)$ to be the label of that third disk. We may continue to define $d(N-2), d(N-3), \ldots$ by the same procedure, specifically,

$$d(i) = \begin{cases} p(i+1) & \text{if } p(i+1) = d(i+1), \\ X \text{ with } p(i+1) \neq X \neq d(i+1) & \text{if } p(i+1) \neq d(i+1). \end{cases}$$

We shall use induction on the number of disks to show that the minimum number of moves is given by summing powers of 2 over just those values of i for which $p(i)$ differs from $d(i)$, that is,

$$\sum_{\substack{1 \leqslant i \leqslant N \\ p(i) \neq d(i)}} 2^{i-1}.$$

Proof. For $N = 1$, when $p(1) = d(1)$, no moves are required and the sum has no terms; when $p(1) \neq d(1)$, we need one move as given by the term 2^0. This serves as the base of the induction.

Assume we have already verified the formula for N disks and consider a system of $N+1$ disks. If it happens that $p(N+1) = d(N+1)$, we ignore that largest disk and simply solve the N disk problem. By induction, the formula has already been verified. But if $p(N+1) \neq d(N+1)$, we observe that to solve the problem we must first stack the N smallest disks onto peg X with $p(N+1) \neq X \neq d(N+1)$, then we must move disk $N+1$ to $d(N+1)$, and finally we must move the stack of N disks also onto $d(N+1)$. Now once we have defined $d(N) = X$, the rules for defining $d(i)$ for all smaller i are identical for the $N+1$ disk problem and for the N disk problem. Thus, the number of moves needed to stack the first N disks is given by

$$\sum_{\substack{1 \leqslant i \leqslant N \\ p(i) \neq d(i)}} 2^{i-1}.$$

Next, we transfer disk $N+1$ in one move, and finally we move the stack of N in $2^N - 1$ moves. Adding these two terms we find that the summation must be augmented by $1 + 2^N - 1 = 2^N$. But this is precisely the term included when we extend the summation to include $i = N+1$. This completes the proof by induction.

When we apply this formula to the conditions stated in the original problem, we find that there is a pattern that repeats every 6 rows:

Disk number	Starting Position	Destination	Contributed Term
$2n$	B	C	2^{2n-1}
$2n-1$	A	B	2^{2n-2}
$2n-2$	B	B	0
$2n-3$	A	C	2^{2n-4}
$2n-4$	B	A	2^{2n-5}
$2n-5$	A	A	0
$2n-6$	B	C	2^{2n-6}

Summing these terms when $2n \equiv r \pmod 3$, with $0 \leqslant r \leqslant 2$, we find that the formula reduces to

$$\tfrac{5}{7}(2^{2n} - 2^{r}) + r.$$

An interesting observation is that the average number of moves needed from any starting position to any of the possible destinations is $(2/3)(2^N - 1)$. To show this, notice that from any starting position there are three possible objectives, namely, $d(N) = A$, B, or C. Now one of these matches $p(N)$ and so is repeated as $d(N-1)$. The other two do not match, which forces them to be interchanged at $d(N-1)$. Thus, the three variants of $d(N-1)$ also comprise all three letters. In this way we find in turn that each $d(i)$ must be comprised of the three possible letters in the three variations. Consequently, if we total the number of moves given by

$$\sum_{\substack{1 \leqslant i \leqslant N \\ p(i) \neq d(i)}} 2^{i-1}$$

for all three versions, we get $2\sum_{i=1}^{N} 2^{i-1} = 2(2^N - 1)$. The average is just this divided by 3.

Also solved by Martin Bazant, Duane M. Broline, Seth Catlin, Con Amore Problem Group (Denmark), Kevin Ford (student), Lorraine L. Foster, William E. Gould and Douglas B. Tyler, Jerrold W. Grossman, John G. Heuver (Canada), R. High, Andreas S. Hinz (Germany), Richard Johnsonbaugh, Richard Laatsch, Sandor Lenoczky (student), Robert Lindahl, P. S. Nair and S. T. Sarasamma, Stephen G. Penrice, Lorel Preston and Elizabeth Brown and Robert Stokes, Flauren Ricketts, Philip Straffin, Wim Vallenduuk (Holland), Jack V. Wales, Jr., Western Maryland College Problems Group, and the proposer. There were four incorrect solutions.

Johnsonbaugh and *Hinz* noted that the solution follows directly from Theorem 3 (page 301) in Andreas M. Hinz, The Tower of Hanoi, *L'Enseignement Mathématique* 35 (1989), 289–321.

Configuration of Perpendiculars — June 1990

1351. *Proposed by Florin S. Pîrvănescu, Slatina, Romania.*

In the acute triangle ABC, let D be the foot of the perpendicular from A to BC, let E be the foot of the perpendicular from D to AC, and let F be a point on the line segment DE. Prove that AF is perpendicular to BE if and only if $FE/FD = BD/DC$.

Solution by Eugene Lee, Boeing Commercial Airplanes, Seattle, Washington.

The proposition is true in general, without the acute triangle requirement.

Let $XY \equiv Y - X$ be the vector from X to Y, with length $|XY|$, and let $\overline{XY}$ denote the line through X and Y, and $\langle XY \rangle$ the segment between X and Y. The general proposition can be stated as follows (after the definitions of D and E). Suppose

$D \neq C$. Let $F \in \overline{DE}$, then $AF \cdot BE = 0$ if and only if F divides $\langle ED \rangle$ in the same way as D divides $\langle BC \rangle$, that is, if and only if

$$\frac{BD \cdot BC}{DC \cdot BC} = \frac{EF \cdot ED}{FD \cdot ED}. \tag{1}$$

Of course (1) implies $|BD|/|DC| = |FE|/|FD|$, but additionally it shows that $D \in \langle BC \rangle$ if and only if $F \in \langle DE \rangle$, hence it uniquely locates the point F on the line $\overline{DE}$.

Proof. Let $F = \lambda D + (1-\lambda)E$ for some real λ. Then $FE = \lambda DE$, $DF = (1-\lambda)DE$, and so (since $D \neq E$),

$$(1-\lambda)FE = \lambda DF. \tag{2}$$

Now $AF = \lambda AD + (1-\lambda)AE$ and $BE = BD + DE$. Since $AD \perp BD$ and $AE \perp DE$, we have $AF \cdot BE = \lambda AD \cdot DE + (1-\lambda)BD \cdot AE$, which will be zero if and only if

$$(1-\lambda)BD \cdot AE = \lambda AD \cdot ED. \tag{3}$$

It is clear that the triangles AED and DEC are similar. From this we get immediately

$$AD \cdot ED = DC \cdot AE,$$

hence (3) becomes

$$(1-\lambda)BD \cdot AE = \lambda DC \cdot AE.$$

Since B, C, D are collinear, and $AE \cdot BC \neq 0$, this can be replaced by

$$(1-\lambda)BD = \lambda DC. \tag{4}$$

Since also E, F, D are collinear, (2) and (4) are clearly equivalent to (1).

Remark. The degenerate case where $D = C$ is also subsumed under the above formulation, if we take for $\overline{DE}$ the limiting line $\overline{BC}$ and if in (1), ED is replaced by a vector in the limiting position, say BC. Then, by (1), $F = D$.

Also solved by Seung-Jin Bang, Leon Bankoff, Duane Broline, Athanasiadis Christos (student), Con Amore Problem Group (Denmark), Ragnar Dybvik (Norway), Jiro Fukuta (Japan), John F. Goehl, Jr., H. Guggenheimer, Francis M. Henderson, John G. Heuver (Canada), Geoffrey A. Kandall, Václav Konečný, Lamar University Problem Solving Group, Kee-Wai Lau (Hong Kong), N. T. Lord (England), Helen M. Marston, Naresh Menon (student), Werner Raffke (Germany), Volkhard Schindler (Germany), John S. Sumner, R. S. Tiberio, Michael Vowe (Switzerland), Staffan Wrigge (Sweden), Robert L. Young, and the proposer.

Bankoff noted that this problem is a generalization of problem E1476, which first appeared in the *American Mathematical Monthly* 69 (1962), 233, with three published solutions based on synthetic, analytic, and vector methods. The problem reappeared in this MAGAZINE, September 1984, as **1199**, with two solutions in the September 1985 issue, one synthetic and the other projective. Additional references are given in the editorial comments to 1199.

Concurrent Lines and Acute Angles **June 1990**

1352. *Proposed by Mark Krusemeyer, Carleton College, Northfield, Minnesota.*

a. Suppose three lines are drawn independently and in random directions through the origin in the plane. (The lines will each extend in two opposite directions from the origin; "random" means that given two equal angles with vertex at the origin, each line is equally likely to be inside one as inside the other.) What is the probability that all the angles formed at the origin by adjacent pairs of lines will be acute? (For example, if the lines are $y=0, y=x, y=2x$, then the angle formed by $y=2x$ and $y=0$ as an adjacent pair of lines at the origin will not be acute. However, if the lines are $y=0, y=2x, y=-2x$, then all angles at the origin will be acute.)

b. Same question, with "three lines" replaced by "n lines."

I. *Solution by Bruce R. Johnson, University of Victoria, British Columbia, Canada.*

We will show that the answer for part b is $1-n/2^{n-1}$; in particular, the answer for part a is $1/4$.

With probability one, no two lines will coincide, so the n lines through the origin will create n pairs of nonoverlapping angles that radiate from the origin and sum to 2π radians. To distinguish the n lines we arbitrarily label them from 1 to n, and for $j \in \{1,2,\dots n\}$ we call the pair of angles formed by line j and the adjacent line on the counterclockwise side of line j, angle pair j. Let O_j denote the event that angle pair j is obtuse. Since at most one angle pair can be obtuse, the events $O_1, O_2, \dots, O_n$ are mutually exclusive. Thus, the probability we seek is

$$Pr(2n \text{ acute angles}) = 1 - Pr(O_1 \cup O_2 \cup \cdots \cup O_n) = 1 - \sum_{j=1}^{n} Pr(O_j).$$

Also, for any j the event O_j will occur if and only if each of the $(n-1)$ angles measured counterclockwise from line j to the other lines is between $\pi/2$ and π radians. Since these $(n-1)$ angles are distributed independently and uniformly over the interval $(0,\pi)$, we have $Pr(O_j) = (1/2)^{n-1}$, and hence

$$Pr(2n \text{ acute angles}) = 1 - \frac{n}{2^{n-1}}.$$

II. *Solution by Con Amore Problem Group, Royal Danish School of Educational Studies, Copenhagen, Denmark.*

Let the lines, in counterclockwise order, be $L_1, L_2, \dots, L_n$. Let $\alpha_1\pi, \alpha_2\pi, \dots \alpha_n\pi$ be the counterclockwise angles between L_1 and L_2, L_2 and $L_3, \dots, L_n$ and L_1, respectively. Then $\alpha_1, \alpha_2, \dots, \alpha_n \geqslant 0$, and $\alpha_1+\alpha_2+\cdots+\alpha_n=1$, and the possible ordered n-tuples $(\alpha_1, \alpha_2, \dots, \alpha_n)$ are precisely the n-tuples of barycentric coordinates of points in an (arbitrarily chosen) $(n-1)$-dimensional (ordered) simplex $S = A_1A_2 \cdots A_n$. Our problem, then, is to find the probability that a point chosen at random from S will have all its barycentric coordinates less than $1/2$.

Now, saying that $\alpha_1 < 1/2$ is equivalent to saying that our point is nearer to the facet $A_2 \cdots A_n$ of S than to the vertex A_1, or in other words, that our point is *not* in the simplex produced by multiplying S by $1/2$ with respect to A_1. Interpreting the conditions $a_2 < 1/2, \dots, \alpha_n < 1/2$ similarly, we see that we are looking for the probability that a random point in S is not in any of the simplices produced by multiplying S by $1/2$ with respect to one of its n vertices. Clearly, this probability is

$$1 - n\left(\tfrac{1}{2}\right)^{n-1}$$

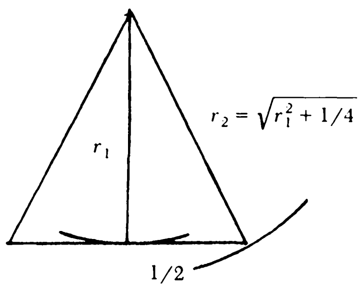
In particular, for $n=3$, the probability is $1/4$. (Note that, as one might expect, the probability converges to 1 for $n \to \infty$.)

Also solved by Duane Broline, David Callan, Curtis Cooper, Kristina Hansen, Philip Straffin, John S. Sumner and Kevin L. Dove, University of Arizona Problem Solving Lab (part a only), and the proposer. A partial solution to b was received as well. Most solutions used multiple integrals.

Answers

Solutions to the Quickies on page 198.

A778. The area is $\pi/4$, regardless of the number of sides of the n-gon. To see why, consider the following figure.



$$\pi r_2^2 - \pi r_1^2 = \pi/4.$$

A779. Let S be the given sum and $T = a + b + c + d + e + f$. Then,

$$S > a/T + b/T + c/T + d/T + e/T + f/T = 1.$$

That 1 is the best possible bound follows by choosing

$$a = 1/\varepsilon^6,\ b = 1/\varepsilon^5,\ c = 1/\varepsilon^4,\ d = 1/\varepsilon^3,\ e = 1/\varepsilon^2, \text{ and } e = 1/\varepsilon,$$

where $\varepsilon << 1$.

The least upper bound is 3 and follows from

$$\frac{a}{f+a+b} + \frac{b}{a+b+c} \le \frac{a+b}{a+b} = 1,$$

$$\frac{c}{b+c+d} + \frac{d}{c+d+e} \le \frac{c+d}{c+d} = 1,$$

$$\frac{e}{d+e+f} + \frac{f}{e+f+a} \le \frac{e+f}{e+f} = 1.$$

The 3 bound is achievable by either setting $a = c = e = 0$ or else by setting $b = d = f = 0$.

A780. If $x > 0$, then $x^{x-1} \geqslant 1 \geqslant x^{1/x-1}$. Thus

$$\begin{aligned}(a/b)^{a/b}(b/c)^{b/c}(c/a)^{c/a} &= (a/b)^{a/b-1}(a/b)(b/c)^{b/c-1}(b/c)(c/a)^{c/a-1}(c/a)\\ &= (a/b)^{a/b-1}(b/c)^{b/c-1}(c/a)^{c/a-1}\\ &\geqslant 1\\ &\geqslant (a/b)^{b/a-1}(b/c)^{c/b-1}(c/a)^{a/c-1}\\ &= (a/b)^{b/a}(b/a)(b/c)^{c/b}(c/b)(c/a)^{a/c}(a/c)\\ &= (a/b)^{b/a}(b/c)^{c/b}(c/a)^{a/c}.\end{aligned}$$

REVIEWS

PAUL J. CAMPBELL, *editor*
Beloit College

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.

CORRECTION. Vaughn F.R. Jones, winner of a 1990 Fields Medal, advises that the Fields Medal does carry a monetary award: each 1990 medalist received Cdn $15,000.

Kolata, Gina, What if they closed 42d Street and nobody noticed?, *New York Times* (25 December 1990) 38. Cohen, Joel E., and Frank P. Kelly, A paradox of congestion in a queueing network, *Journal of Applied Probability* 27 (1990) 730–734.

Adding capacity or a new route to a network would seem always to be advantageous to network users, particularly if the network is already congested. Not true! In fact, if a new route is added to a *congested* transportation network, the situation can get worse for every user, a fact discovered in 1968 by Dietrich Braess (Institute for Numerical and Applied Mathematics, Münster) and now known as *Braess's paradox*. Cohen and Kelly note that traffic in downtown Stuttgart in the 1960s got worse after a street was added, and improved after it was closed; and Kolata observes that traffic flow in New York improved while 42nd St. was closed during Earth Day in 1990. Braess's model was deterministic, but Cohen and Kelly give a queueing network model in which the paradox occurs. In the traffic example given by Kolata (and adapted from Cohen and Kelly), two streams of traffic have a common destination: opening a diagonal route from one to the other allows traffic taking it to help congest both original routes. For all users, average travel time increases. "Self-seeking individuals are unable to refrain from using the additional capacity, even though using it leads to deterioration in the mean transit time," say Cohen and Kelly.

Cipra, Barry A., The breaking of a mathematical curse, *Science* 251 (11 January 1991) 165.

Numerical integration over n dimensions, for an "average" function and to a specified average error, seems to require an amount of computation exponential in n. However, Henryk Woźniakowski (Columbia University) realized that the multivariate integration problem translates into another problem known as *L_2 discrepancy*, for which a solution algorithm already exists. Translating the solution back in to the language of integration revealed that with the right choice of points (which the solution algorithm also prescribes), the number of points needed is almost independent of n.

Cipra, Barry A., Mathematics—amid war—in San Francisco, *Science* 251 (8 February 1991) 628–629.

Notes that at the recent AMS/MAA Joint Mathematics Meetings in San Francisco, a number of topics came up that "would have been unusual at a mathematics meeting a few years ago." Hector Sussman (Rutgers University) summarized the state of control theory (on which theory "smart" bombs rely). Celebration of the 20th anniversary of the founding of the Association for Women in Mathematics brought forth reflections on the outlook for women in mathematics. And mathematics continues as a source for computer and human art.

Miller, Donald L., and Joseph F. Pekny, Exact solution of large asymmetric traveling salesman problems, *Science* 251 (15 February 1991) 754–761.

The traveling salesman problem is NP-hard. The authors give an exact algorithm for optimal solutions to the traveling salesman problem with *asymmetric* intercity costs, which finds solutions to random asymmetric problems with 5,000 cities in a few seconds and with 500,000 cities in a few hours. The algorithm reported is used to generate schedules for a variety of chemical manufacturing facilities, a problem for which asymmetric costs are typical. Learning why this algorithm is not as effective on symmetric problems requires close analysis of the paper.

Kolata, Gina, Math problem, long baffling, slowly yields, *New York Times* (12 March 1991) C1, C9.

The record-largest traveling salesman problem that has been solved exactly is one with 2,392 cities; researchers are now competing to solve a 3,038- city problem. Traveling salesman problems of enormous size arise in the fabrication of circuit boards and very large-scale integrated circuits, in which as many as a million holes ("cities") need to be drilled. For a million-city tour, it now takes about 3.5 hours of computing to get an answer that is within 3.5% of optimal, and seven months to get within 0.75%.

Moffatt, Anne Simon, Early detection nips math problems in the bud, *Science* 251 (8 March 1991) 1173–1174.

Reports on the great success of the Ohio Early College Mathematics Placement Program, now used by school systems in 15 other states too. The Program tests a high-school junior's mathematics knowledge and compares it to the mathematics needed in the careers to which the student aspires. The student's senior year can be used to address deficiencies. The Program has "halved the need for remedial math courses in Ohio's major colleges and universities."

Peterson, Ivars, Finding fault: the formidable task of eradicating software bugs, *Science News* 139 (16 February 1991) 104–106.

The Darlington Nuclear Generating Station, the first Canadian nuclear power plant to use computers to operate its two emergency shutdown systems, will begin operation in 1992. To prove mathematically the correctness of the 10,000 lines of code for each shutdown system has taken about three years. The article also details the software failure that caused disruption of AT&T's long-distance network in January, 1990.

Ascher, Marcia, *Ethnomathematics: A Multicultural View of Mathematical Ideas*, Brooks/-Cole, 1991; ix + 203 pp. ISBN 0-534-14880- -8

A splendid book well worth reading, using in courses, and loaning to friends who think they don't like mathematics. It stresses the intimate link between culture and the broader realm of mathematical ideas (as opposed to just mathematics). Chapters treat mathematical ideas from "traditional" cultures around the world, with particular attention to the peoples of Oceania; the book complements rather than overlaps Claudia Zaslavsky's *Africa Counts: Number and Pattern in African Culture* (1973). Topics treated include number words and symbols, unicursal networks, the logic of kin relations, chance and strategy in games and puzzles, space, symmetric strip decorations. The book is replete with notes and references to other sources (unfortunately, the index ignores the notes); instructors using it as a text will need to devise their own exercises and projects.

Higham, Nicholas J., Is fast matrix multiplication of practical use?, *SIAM News* (November 1990) 12, 14.

It has been more than 20 years since V. Strassen discovered a method for multiplying two $n \times n$ matrices which requires at most $4.7n^{\log_2 7} \approx 4.7n^{2.8}$ arithmetic operations instead of $O(n^3)$ operations. The current record, achieved in 1987 by D. Coppersmith and S. Winograd, is that matrix multiplication can be done in $O(n^{2.376})$ operations. But all this is theory—how practical are these "fast" multiplications? Strassen's method has been shown to be faster than conventional multiplication by a factor of 1.45 for $n = 128$ and a factor of 2.01 for $n = 2{,}048$ (with one-third of the speedup due to techniques peculiar to a Cray 2 supercomputer). Moreover, although "Strassen's method is not as stable as conventional multiplication... it is stable enough to be a contender for practical use." And to whom does this matter? Many researchers now commonly solve dense systems of 10,000 or more linear equations. This fine summary of the state of research in fast matrix multiplications includes a full bibliography of the relevant papers.

Higham, Nick, and Nick Trefethen, Complete pivoting conjecture is disproved, *SIAM News* 24(1) (January 1991) 9.

"The growth factor in Gaussian elimination is the ratio of the largest number that appears at any stage of the elimination to the largest element in the original matrix. J.H. Wilkinson's backward analysis of the early 1960s showed that Gaussian elimination is numerically stable as long as the growth factor remains small." In 1968 C. Cryer had conjectured that the growth factor for elimination with complete pivoting, applied to an $n \times n$ real matrix, is bounded by n. (In complete pivoting, the largest element from the whole remaining active submatrix is taken as the pivot, so that both row and column interchanges are done.) This "complete pivoting conjecture" has now been disproved by Nick Gould (Atlas Centre, Rutherford Appleton Laboratory, England), who found a 13×13 matrix for which the growth factor is 13.0205. For comparison, the algorithm used in practice (and taught in linear algebra courses as the desirable algorithm), Gaussian elimination with partial pivoting (only rows are interchanged), has worst-case behavior that is "catastrophically unstable" (a growth factor of 2^{n-1}) but has "growth factors of order n or less for all but a tiny proportion of matrices."

Schroeder, Manfred, *Fractals, Chaos, Power Laws: Minutes from an Infinite Paradise*, Freeman, 1991; xii + 429 pp, $32.95. ISBN 0- 7167-2136-8

"The unifying concept underlying fractals, chaos, and power laws is self-similarity.... Self-similarity is one of the decisive symmetries that shape our universe and our efforts to comprehend it." Such a richness of topics and amazing splendor of illustrations! Fractals, scaling laws, chaos, strange attractors, percolation, Cayley trees, Morse-Thue sequences, mode locking, quasicrystals—here are many of the exciting topics of contemporary mathematics. Introducing students to contemporary mathematics early in their college careers (e.g., their first term) would go a long way toward promoting appreciation for mathematics and stimulating interest in mathematics as a living subject worth the devotion of a career.

Schroeder's prose, too, in places far surpasses the ordinary: "Neither tori, nor *cantori*, nor Arnold tongues will faze us as we (sur)mount devil's staircases to unwind among the rational winding numbers festooning Farey trees" (p. xvi).

Folger, Tim, Shuffling into hyperspace. *Discover* 12:1 (January 1991) 66–67.

Seven riffle shuffles suffice to randomize a pack of cards. This article gives further details of the ideas behind the several-years-old proof by Persi Diaconis (Harvard) and David Bayer (Columbia).

Wallich, Paul, Garbage in, garbage out. *Scientific American* (December 1990) 126.

Computer programs for geometric modeling, such as CAD (computer-aided design) programs, suffer from the inherent inexactness of representation of numbers in floating-point arithmetic. The computer representations of points that lie on a surface or within a region may not do so, and erroneous results or a computer crash may result. Greater precision doesn't help. A promising approach is to introduce logic to maintain consistency between the geometrical relationships of the ideal points and the numerical relationships of their computer representations.

Peterson, Ivars, Equations in stone: A mathematician turns to sculpture to convey the beauty of mathematics. *Science News* 138 (8 September 1990) cover, 152–154.

Helaman Ferguson is a mathematician (Brigham Young University) whose sculptures of mathematical objects were exhibited at the 75th Anniversary Meeting of the MAA in Columbus, Ohio. A brief note appeared in the January-February issue of *Focus* to note the opening of his exhibit at MAA headquarters. The article in *Science* gives more background about the artist and what he is trying to do. To reflect the permanence of mathematical theorems, Ferguson prefers to work in materials that will survive on a geological scale, viz., stone. Says he, "I am interested in the adventures of affirming pure mathematical thought in unpredictable physical form." Details of the mathematics are given in an article by Ferguson in the December 1990 issue of the *American Mathematical Monthly*.

Cipra, Barry, Big number breakdown. *Science* 248 (29 June 1990) 1608. Folger, Tim, Most-wanted number. *Discover* 12:1 (January 1991) 67.

In 1990, the "most-wanted" integer, the 155-digit Fermat number $F_9 = 2^{512}+1$, was factored by using the ***number field sieve*** invented by John Pollard. Closely related to the quadratic sieve, the number field sieve breaks down the original factoring problem over the integers into a great many factoring problems in an algebraic number field. The factoring of F_9 took two months on 1,000 computers around the world; to factor F_{10}, which has 309 digits, might take "half a million times the resources."

Apostolakis, George, The concept of probability in safety assessments of technological systems. *Science* 250 (7 December 1990) 1359–1364.

Discusses how to use Bayesian methods to incorporate expert opinions into probabilistic risk assessment. Probability is not interpreted as relative frequency but as a measure of degree of belief. "Physical scientists and engineers... are uncomfortable with the extensive use of judgment...." The author acknowledges that the question of selecting the experts "falls outside of the mathematical theory."

NEWS AND LETTERS

NINETEENTH ANNUAL U.S.A. MATHEMATICAL OLYMPIAD PROBLEMS AND SOLUTIONS

1. A certain state issues license plates consisting of six digits (from 0 through 9). The state requires that any two plates differ in at least two places. (Thus the plates 027592 and 020592 cannot both be used.) Determine, with proof, the maximum number of distinct license plates that the state can issue.

Solution. The state can issue 10^5 license plates. One method for doing so is to use a "check digit," as follows. For each of the 10^5 five-digit strings $x_1x_2x_3x_4x_5$, define x_6 so that

$$x_6 \equiv x_1 + x_2 + x_3 + x_4 + x_5 \pmod{10}.$$

For any pair of distinct strings

$$a_1a_2a_3a_4a_5a_6 \text{ and } b_1b_2b_3b_4b_5b_6$$

constructed in this way, there must be at least one position j with $1 \leq j \leq 5$ such that $a_j \neq b_j$. But if there is only one such j, then

$$\begin{aligned} a_6 - b_6 &\equiv (a_1+a_2+a_3+a_4+a_5) \\ &\qquad - (b_1+b_2+b_3+b_4+b_5) \\ &= a_j - b_j \\ &\not\equiv 0 \pmod{10}, \end{aligned}$$

so $a_6 \neq b_6$. Hence $a_1a_2a_3a_4a_5a_6$ and $b_1b_2b_3b_4b_5b_6$ must differ in at least two places.

To show that no method can produce a greater number of acceptable license plates, observe that among $10^5 + 1$ distinct license plates, two would have to agree in their first 5 places, where only 10^5 distinct combinations are possible. These two license plates would differ in only one place.

2. A sequence of functions $\{f_n(x)\}$ is defined recursively as follows:

$$f_1(x) = \sqrt{x^2 + 48}, \text{ and}$$
$$f_{n+1}(x) = \sqrt{x^2 + 6f_n(x)} \quad \text{for } n \geq 1.$$

(Recall that $\sqrt{}$ is understood to represent the positive square root.) For each positive integer n, find all real solutions of the equation $f_n(x) = 2x$.

Solution. Observe first that $f_n(x)$ is positive for every n and every x, so $f_n(x) = 2x$ admits only positive solutions.

We show that, for each n, the unique solution of $f_n(x) = 2x$ is $x = 4$. To begin, we first prove by induction on n that $x = 4$ is a solution. For $n = 1$ we have $f_1(4) = \sqrt{16+48} = 2\cdot 4$. Suppose that $f_k(4) = 2\cdot 4$. Then $f_{k+1}(4) = \sqrt{16+6f_k(4)} = \sqrt{16+48} = 2\cdot 4$, completing the induction.

To see that there are no other solutions, we show by induction that,

(*) For each n, $\dfrac{f_n(x)}{x}$ decreases as x increases in $(0, \infty)$, and therefore cannot take on the value 2 more than once.

With $n = 1$ we have $\dfrac{f_1(x)}{x} = \sqrt{1 + \dfrac{48}{x^2}}$, which decreases as x increases. Now suppose that $\dfrac{f_k(x)}{x}$ decreases as x increases. Then

$$\frac{f_{k+1}(x)}{x} = \sqrt{1 + \frac{6}{x} \cdot \frac{f_k(x)}{x}}$$

also decreases as x increases, and the proof of (*) is complete.

3. Suppose that necklace $\mathcal{A}$ has 14 beads and necklace $\mathcal{B}$ has 19. Prove that, for every odd integer $n \geq 1$, there is a way to number each of the 33 beads with an integer from the sequence

$$\{n, n+1, n+2, \ldots, n+32\}$$

so that each integer is used once, and adjacent beads correspond to relatively prime integers. (Here a "necklace" is viewed as a circle in which each bead is adjacent to two other beads.)

Solution. We take an integer m, $1 \leq m \leq 18$, and number the beads of necklace $\mathcal{A}$ with the consecutive integers

$$n+m, n+m+1, \ldots, n+m+13.$$

We have to join the ends of this chain together, which is allowed so long as $n+m$ and $n+m+13$ are relatively prime; i.e.,

$$\gcd(n+m, n+m+13) = 1.$$

(Since pairs of consecutive positive integers are always relatively prime, no other conditions on necklace $\mathcal{A}$ are necessary.)

Next, we number the beads of necklace $\mathcal{B}$ with the consecutive integers from $n+m+14$ to $n+32$ (note that $m+14 \le 32$), and then follow $n+32$ with n and continue up to $n+m-1$. Again, all pairs of consecutive positive integers are relatively prime, so the numbering will succeed provided that the following two conditions are satisfied:

$$\gcd(n, n+32) = 1, \text{ and}$$
$$\gcd(n+m-1, n+m+14) = 1.$$

Thus, since $\gcd(a,b) = \gcd(a, b-a)$, the numbering method is valid if

$$\gcd(n,32) = \gcd(n+m-1,15) = \gcd(n+m,13) = 1.$$

The first of these conditions holds automatically, since n is given as odd. The second condition (modulo 15) is equivalent to corresponding conditions modulo 3 and modulo 5. Therefore, the numbering succeeds if m can be chosen such that

$$m \not\equiv 1-n \pmod 3,$$
$$m \not\equiv 1-n \pmod 5,$$
$$m \not\equiv -n \pmod{13}.$$

Out of the 18 consecutive possible values for m:

only 6 will have $m \equiv 1-n \pmod 3$,
at most 4 will have $m \equiv 1-n \pmod 5$, and
at most 2 will have $m \equiv -n \pmod{13}$.

This leaves at least $18-(6+4+2) = 6$ values of m satisfying all the requirements for the numbering scheme.

Note. The interval $1 \le m \le 18$ can be replaced by certain shorter intervals; e.g., $1 \le m \le 5$.

4. Find, with proof, the number of positive integers whose base-n representation consists of distinct digits with the property that, except for the leftmost digit, every digit differs by ± 1 from some digit further to the left. (Your answer should be an explicit function of n in simplest form.)

Solution. Suppose that a base-n integer with distinct digits has leftmost digit d, exactly j digits less than d, and exactly k digits greater than d, where

$$1 \le d \le n-1,$$
$$0 \le j \le d, \quad \text{and}$$
$$0 \le k \le n-d-1.$$

Such an integer will satisfy the conditions of the problem if and only if:

(1) the j digits less than d are $d-1$, $d-2$, ..., $d-j$, and these digits appear from left to right in the order listed;

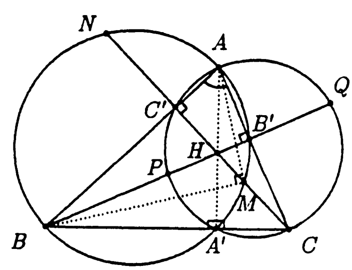
(2) the remaining k digits are $d+1$, $d+2$, ..., $d+k$, and these also appear in the order listed.

Since the orderings of the digits are fixed within these increasing and decreasing subsequences, a suitable integer arises uniquely from each of the $\binom{j+k}{j}$ possible choices of j positions for subsequence (1) from among the $j+k$ positions to the right of d. Therefore, the total number of suitable base-n integers is $\sum_{d=1}^{n-1} \sum_{j=0}^{d} \sum_{k=0}^{n-d-1} \binom{j+k}{j}$

$$= \sum_{d=1}^{n-1} \sum_{j=0}^{d} \binom{j+n-d}{j+1}$$
$$= \sum_{d=1}^{n-1} \left[\binom{n+1}{d+1} - 1 \right]$$
$$= \sum_{r=0}^{n+1} \binom{n+1}{r} - \binom{n+1}{0} - \binom{n+1}{1} - \binom{n+1}{n+1} - (n-1)\cdot 1$$
$$= 2^{n+1} - 1 - (n+1) - 1 - (n-1)$$
$$= 2^{n+1} - 2 - 2n.$$

5. An acute-angled triangle ABC is given in the plane. The circle with diameter AB intersects altitude CC' and its extension at points M and N, and the circle with diameter AC intersects altitude BB' and its extension at P and Q. Prove that the points M, N, P, Q lie on a common circle.

Solution.



The perpendicular bisectors of MN and PQ are AB and AC, respectively, so if M, N, P, Q do lie on a circle, the center can only be point A. Since we already have $AM = AN$ and $AP = AQ$, we have only to prove $AM = AP$.

Point C' is the foot of the altitude to the hypotenuse of right triangle ABM; therefore,

$$AM^2 = AB \cdot AC' = AB \cdot AC \cos \angle BAC.$$

Similarly,

$$AP^2 = AC \cdot AB' = AC \cdot AB \cos \angle BAC.$$

Thus $AM = AP$ completing the problem.

THIRTYFIRST ANNUAL INTERNATIONAL MATHEMATICAL OLYMPIAD PROBLEMS

1. Chords AB and CD of a circle intersect at a point E inside the circle. Let M be an interior point of the segment EB. The tangent line at E to the circle through D, E, and M intersects the lines BC and AC at F and G, respectively.

If $\frac{AM}{AB} = t$, find $\frac{EG}{EF}$ in terms of t.

2. Let $n \geq 3$ and consider a set E of $2n-1$ distinct points on a circle. Suppose that exactly k of these points are to be colored black. Such a coloring is "good" if there is at least one pair of black points such that the interior of one of the arcs between them contains exactly n points from E. Find the smallest value of k so that every such coloring of k points of E is good.

3. Determine all integers $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer.

4. Let $\mathbf{Q}^+$ be the set of positive rational numbers. Construct a function $f\colon \mathbf{Q}^+ \to \mathbf{Q}^+$ such that $f(x f(y)) = \frac{f(x)}{y}$ for all x, y in $\mathbf{Q}^+$.

5. Given an initial integer $n_0 > 1$, two players, $\mathcal{A}$ and $\mathcal{B}$, choose integers $n_1, n_2, n_3, \ldots$ alternately according to the following rules:

Knowing n_{2k}, $\mathcal{A}$ chooses any integer n_{2k+1} such that $n_{2k} \leq n_{2k+1} \leq n_{2k}^2$.

Knowing n_{2k+1}, $\mathcal{B}$ chooses any integer n_{2k+2} such that $\frac{n_{2k+1}}{n_{2k+2}}$ is a prime raised to a positive integer power.

Player $\mathcal{A}$ wins the game by choosing the number 1990; player $\mathcal{B}$ wins by choosing the number 1. For which n_0 does:

(a) $\mathcal{A}$ have a winning strategy?

(b) $\mathcal{B}$ have a winning strategy?

(c) neither player have a winningstrategy?

6. Prove that there exists a convex 1990-gon with the following two properties:

(a) All angles are equal.

(b) The lengths of the sides are the numbers $1^2, 2^2, 3^2, \ldots, 1990^2$ in some order.

The 1990 U.S.A. Mathematical Olympiad was prepared by Douglas Hensley, Gerald Heuer, Gregg Patruno, Bjorn Poonen, Ian Richards (chair), Leo Schneider, and Daniel Ullman.

The top eight students in the 1990 USAMO were: Kiran S. Kedlaya, Silver Spring, MD; Jeffrey M. Vanderkam, Raleigh, NC; Hugh A. Thomas, Winnipeg, MB; János Csirik, Victoria, BC; Daniel R. Brown, Willowdale, ON; Joel E. Rosenberg, West Hartford, CT; Royce Y. Peng, Rancho Palos Verdes, CA; and Jonathan T. Higa, Honolulu, HI.

The U.S.A. placed third at the 31st International Mathematical Olympiad in July, 1990 in Beijing, China. Members of the USA team were Avinoam Freedman (Teaneck, NJ), Kiran Kedlaya, Timothy Kokesh (Bartlesville, OK), Royce Peng, Joel Rosenberg, and Jeffrey Vanderkam. Kedlaya and Vanderkam received Gold Medals; Freedman, Peng, and Rosenberg received Silver Medals. The training session to prepare the USA team for the IMO was held at the US Naval Academy, Annapolis, MD, and was directed by Gerald Heuer and Gregg Patruno.

The publication *Mathematical Olympiads 1990* presents several additional solutions to problems on the 19th USA Mathematical Olympiad and solutions to the 31st International Mathematical Olympiad. This booklet is available from:

Dr Walter Mientka
Department of Mathematics
University of Nebraska
Lincoln, NE 68588-0658

Copies are \$2.00 for each year, 1976-1990, with a minimum order of \$6.00, payable in US funds.

Introducing E.Z. Math for the HP 48SX

E.Z. Math is a program for the Hewlett Packard 48SX calculator written, conceived and programmed by Raymond La Barbera and the E.Z. Software Company. It comes on a 128K plug-in ROM card and with a 188 page manual. It is designed to be used by math and science students, teachers, parents and business people.

What Does E.Z. Math Do?

E.Z. Math has six modules dealing with graphs, loans, savings, numbers, games and music:

Graphs. E.Z. Math covers the entire high school and college graphing curriculum, from elementary algebra to advanced calculus. The student can choose from 188 families of equations, inequalities, functions, systems of equations and systems of inequalities, in rectangular, polar and parametric form, all laid out and arranged in an easy-to-use, logically organized system of menus. E.Z. Math makes the graphic analysis of polynomial, rational, trigonometric, hyperbolic, logarithmic and exponential functions quick and easy.

Loans. E.Z. Math makes it easy to solve problems involving fixed rate mortgages on houses, condos, co-ops, and other real estate investments. Anyone wanting to purchase a home can quickly compute the monthly mortgage payment, the amount that can be borrowed, the number of years needed to pay off the loan and the annual interest rate and see a detailed breakdown of each payment in a complete amortization table.

Savings. E.Z. Math makes it easy to solve problems involving a single deposit or repeated deposits to a savings account, certificate of deposit [C.D.], term deposit [T.D.], money market account or other such investment. Anyone interested in saving money can quickly and easily compute the amount accumulated, the amount that must be deposited, the number of years necessary to keep the money on deposit and the annual interest rate.

Numbers. E.Z. Math makes it easy to handle numbers of various types. Elementary and high school students will find it easy to compute all the factors and the prime factorization of a natural number. In addition, finding the greatest common factor, least common multiple and average of any set of natural numbers is a snap. Any set of rational numbers, whether in whole number, fraction or mixed number form, may be added, subtracted, multiplied or divided yielding an answer expressed as a fraction or mixed number in lowest terms or as an integer. Any set of complex numbers may be added, subtracted, multiplied, divided or raised to a power. Any number of terms of the sequences of perfect nth powers, triangular numbers, binomial coefficients, Fibonacci numbers and multiples of a number can be easily computed.

Recreation. E.Z. Math provides a couple of strategy number games and an introduction to the musical capabilities of the HP48SX. These are provided both for fun and as an encouragement to explore further some of the many features of the calculator, including a bit of the built-in rich programming language.

Education. Although using most features of E.Z. Math involves no more than plugging in the ROM card and following the various on-screen menus, the E.Z. Math User's Manual explains very clearly and precisely in complete detail all features and display screens of the program. Just as important, 46 pages of the manual are devoted to simple, intuitive explanations of the basic concepts involved in graphs, numbers, sets, variables, equations, savings and loans.

What's Special About E.Z. Math?

E.Z. Math has many special and unique features which contribute to its practicality and ease of use. Here are some of them:

- A very easy-to-use, logically organized user interface makes possible the full use of all E.Z. Math features without having to open the 850 page HP Owner's Manual.
- To reduce the possibility of user error, all answer screens repeat all entered data when displaying the answer.
- All menu screens, answer screens and graphics screens are easily printable on the HP82240 infrared printer.
- Careful error trapping takes care of invalid user input without crashing the program.
- Absolutely no user contact with the stack is required to use all E.Z. Math features. Yet, going to the stack without quitting E.Z. Math is just a keystroke away.
- Our easy quit feature restores all user system flags and custom menus, leaves no "garbage" on the stack and gets rid of variables which are no longer needed.
- Our easy off feature allows turning off the calculator without quitting the program.

How to Order E.Z. Math

E.Z. Math is available at a retail price of $125.00, plus $5.00 shipping and handling. We accept payment by check, money order, COD, VISA, Mastercard, American Express and school purchase orders. If within 30 days of receipt you find that E.Z. Math fails to fulfill your expectations, we'll gladly take back your copy for a prompt, courteous refund. To order copies of E.Z. Math or to obtain information about about ordering E.Z. Math bundled with HP 48SX calculators and classroom overhead projector kits, please write or call:

SMI Corporation
Dept EMG
250 West New Street, Suite 48
Kingsport, TN 37660
(800) 234-0123 or (615) 378-4821 or (615) 245-8982 (Fax)

CONTENTS

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, NW
Washington, D.C. 20036