MATHEMATICAL SPECTRUM

A MAGAZINE FOR STUDENTS AND TEACHERS OF MATHEMATICS AT SCHOOLS, COLLEGES AND UNIVERSITIES

Volume 23 1990/91 Number 1

Mathematical Spectrum is a magazine for students and teachers in schools, colleges and universities, as well as the general reader interested in mathematics. It is published by the Applied Probability Trust, a non-profit making organisation established in 1963 with the support of the London Mathematical Society. The object of the Trust is the encouragement of study and research in the mathematical sciences.

Volume 23 of *Mathematical Spectrum* will consist of four issues, of which this is the first. Subsequent issues will be published in November 1990, February 1991 and May 1991.

Articles published in *Mathematical Spectrum* deal with the entire range of mathematical disciplines (pure mathematics, applied mathematics, statistics, operational research, computing science, numerical analysis, biomathematics). Both expository and historical material may be included, as well as elementary research and information on educational opportunities and careers in mathematics. There is also a section devoted to problems.

The Editorial Committee welcomes the submission of suitable material, including correspondence, queries and solutions to problems, for publication in *Mathematical Spectrum*. Students are encouraged to send in contributions. All correspondence about the contents should be sent to:

The Editor, Mathematical Spectrum,
Hicks Building, The University, Sheffield S3 7RH

Morley's Theorem

K. R. S. SASTRY, *Box 21862, Addis Ababa, Ethiopia*

Readers may not know of the beautiful theorem about trisecting the angles of a triangle, discovered in 1904 by the Anglo-American mathematician Frank Morley. Start with any triangle ABC and trisect its angles. Denote by P, Q and R the points of intersection of adjacent trisectors, as shown in figure 1. Then PQR is always an equilateral triangle. (See reference 1 for a proof.)

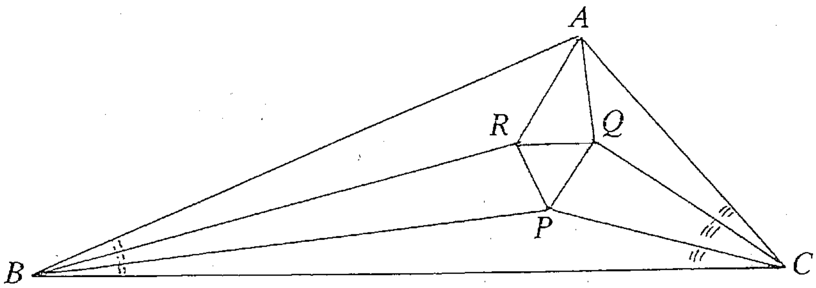


Figure 1

A similar, but much more elementary, result is the following. Start with any rhombus $ABCD$ and k-sect its angles, where k is any integer greater than 2. Let $PQRS$ be the quadrilateral formed by adjacent k-sectors, as shown in figure 2 for the case $k = 3$. Then $PQRS$ is a rectangle. Further, this remains a true statement if we interchange the words 'rhombus' and 'rectangle'. (See figure 3.) Readers should easily be able to convince themselves of the truth of these results.

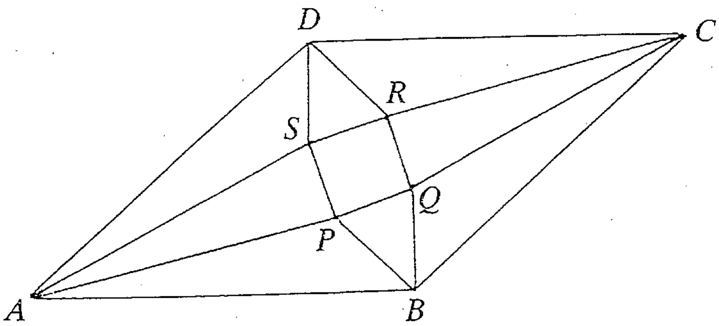


Figure 2

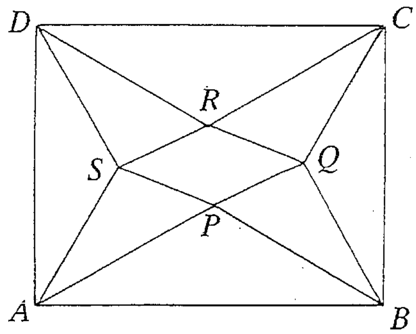


Figure 3

References

1. Ross Honsberger, *Mathematical Gems* I, Dociani Mathematical Expositions (Mathematical Association of America, pages 92–99).

Optimizing the Wait for the Bus: Reflections of a Commuter

WILLIAM WOODSIDE, *Queen's University*
CHRISTIAN T. L. JANSSEN, *University of Alberta*

The authors are both faculty members at Canadian universities. William Woodside is in the Department of Mathematics and Statistics at Queen's University, Kingston, Ontario, and Christian Janssen is in the Department of Finance and Management Science at the University of Alberta in Edmonton.

1. Introduction

The departure time of a bus is a random variable T with probability density function f and distribution function F. If I arrive early I have to wait, suffering discomfort (or cost) at a rate of d units per minute. If I arrive late, I miss the bus and have to make other arrangements which have an associated discomfort (cost) of k units. What is my optimal arrival time if I wish to minimize my expected total discomfort?

Suppose my arrival time is a. If I am early, i.e. if $a < T$, then I wait $T-a$ minutes and my discomfort is $d(T-a)$. If I am late, i.e. if $a > T$, my discomfort is k. Thus my expected total discomfort is

$$D(a) = d\int_a^\infty (t-a)f(t)\ \mathrm{d}t + k\int_{-\infty}^a f(t)\ \mathrm{d}t. \tag{1}$$

I wish to find the value a^* of a which minimizes $D(a)$.

Recalling the rule for differentiating an integral:

$$\frac{\mathrm{d}}{\mathrm{d}x}\int_{u(x)}^{v(x)} g(x,t)\ \mathrm{d}t = \int_{u(x)}^{v(x)} \frac{\partial g}{\partial x}\ \mathrm{d}t + g(x,v(x))v'(x) - g(x,u(x))u'(x)$$

(provided u and v are continuously differentiable and g and $\partial g/\partial x$ are continuous), the derivative of $D(a)$ is

$$D'(a) = -d\int_a^\infty f(t)\ \mathrm{d}t + kf(a)$$

which is zero when

$$\frac{k}{d}f(a) = \int_a^\infty f(t)\ \mathrm{d}t,$$

i.e. when

$$\frac{k}{d}f(a) = 1 - F(a). \tag{2}$$

The second derivative is

$$D''(a) = df(a) + kf'(a),$$

which is positive provided

$$\frac{k}{d} f'(a) > -f(a). \tag{3}$$

Thus the optimal arrival time a^* is any solution of (2) which satisfies the inequality (3). Note that (3) is certainly satisfied when $f'(a)$ is positive, for example when a lies to the left of the modal value of a unimodal distribution.

If T is uniformly distributed over the interval $[0, 1/\lambda]$, it is an easy exercise to show that

$$a^* = \frac{1}{\lambda} - \frac{k}{d},$$

provided this is positive, and zero otherwise. As intuitively expected, the greater the penalty for being late the earlier I should arrive. However, once the penalty exceeds the threshold value d/λ, I should arrive promptly at the beginning of the interval over which T is distributed.

We now consider other possible distributions of T.

2. Gamma distribution

The gamma distribution has probability density

$$f(x) = \frac{\lambda e^{-\lambda x}(\lambda x)^{n-1}}{(n-1)!},$$

with mean $\mu = n/\lambda$ and variance n/λ^2, where n is a positive integer 'shape' parameter. When $n = 1$, the gamma distribution specializes to the exponential distribution. Graphs of the gamma distribution for $n = 1$, 2 and 3 are shown in Figure 1. Equation (2) becomes

$$\frac{k}{d} \frac{\lambda e^{-\lambda a}(\lambda a)^{n-1}}{(n-1)!} = \int_a^\infty \frac{\lambda e^{-\lambda x}(\lambda x)^{n-1}}{(n-1)!}\, dx$$

or

$$\frac{k}{d} e^{-\lambda a} a^{n-1} = \int_a^\infty e^{-\lambda x} x^{n-1}\, dx \tag{4}$$

and inequality (3) becomes, after some simplification

$$n-1 > a\left(\lambda - \frac{d}{k}\right).$$

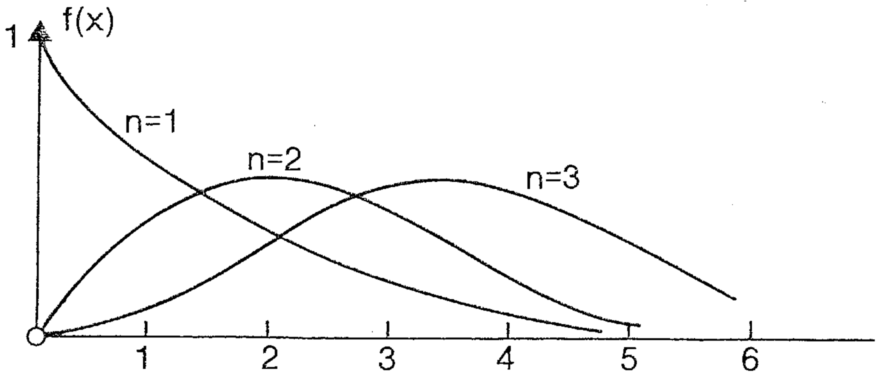


Figure 1. Gamma distribution for $n = 1,2,3$ and $\lambda = 1$

When $n = 1$, and T has a negative exponential distribution, (4) becomes

$$\frac{k}{d}\mathrm{e}^{-\lambda a} = \frac{1}{\lambda}\mathrm{e}^{-\lambda a}$$

which has no solution for a, unless $k/d = 1/\lambda$ when *any* $a \geqslant 0$ is a solution! Returning to (1), the discomfort function $D(a)$ in this case is

$$\begin{aligned} D(a) &= d\int_a^\infty (t-a)\lambda\mathrm{e}^{-\lambda t}\,\mathrm{d}t + k\int_0^a \lambda\mathrm{e}^{-\lambda t}\,\mathrm{d}t, \\ &= k+\left(\frac{d}{\lambda}-k\right)\mathrm{e}^{-\lambda a} \qquad (\text{for } a \geqslant 0). \end{aligned}$$

If $k > d/\lambda$, $D(a)$ is clearly minimized when $\mathrm{e}^{-\lambda a}$ is largest within the allowable interval, i.e. when $a = 0$, and then $D(a) = d/\lambda = \mu d$. If $k = d/\lambda$, $D(a) = k$ for all $a \geqslant 0$ and so, as observed above, any $a \geqslant 0$ is a solution. If $k < d/\lambda$, then $D(a)$ is minimal when $a = +\infty$ and then $D(a) = k$. Thus if the penalty k is less than the expected discomfort one suffers on arriving at $a = 0$, it is better to miss the bus *purposely* and pay the penalty. In summary, if $k > d/\lambda$, I should arrive on time, i.e. at $a^* = 0$; if $k < d/\lambda$, $a^* = +\infty$ and if $k = d/\lambda$ it is immaterial when I arrive.

When $n = 2$, the solution of (4) is

$$a^* = \left[\lambda^2\left(\frac{k}{d}-\frac{1}{\lambda}\right)\right]^{-1}.$$

Note that $a^* \geqslant 0$ provided $k > d/\lambda$. This condition also turns out to be the sufficient condition for a^* to minimize $D(a)$.

When $n = 3$, (4) becomes the quadratic equation

$$\frac{k}{d}a^2 = \frac{a^2}{\lambda} + \frac{2a}{\lambda^2} + \frac{2}{\lambda^3},$$

and it can be shown that

$$a^* = \frac{1+\sqrt{\dfrac{2\lambda k}{d}-1}}{\lambda^2\left(\dfrac{k}{d}-\dfrac{1}{\lambda}\right)}$$

provided $k > d/\lambda$. It is interesting that this last condition also guarantees that a^* is real and positive.

Larger values of n lead to a polynomial equation of degree $n-1$ for a^*. If a_n^* denotes the optimal arrival time when T has a gamma distribution with parameter n and mean n/λ, then, provided $k > d/\lambda$,

$$a_3^* > a_2^* > a_1^* = 0,$$

i.e. as the mean bus departure time increases, the optimal arrival time a^* increases.

3. Normal distribution $N(0, \sigma^2)$

Suppose the departure time is normally distributed with mean 0 and standard deviation σ. Equation (2) now becomes

$$\frac{k}{d}\frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{a^2}{2\sigma^2}\right) = \int_a^{\infty} \frac{1}{\sigma\sqrt{2\pi}}\exp\left(-\frac{x^2}{2\sigma^2}\right) \mathrm{d}x$$

which simplifies to

$$\frac{2}{\sqrt{\pi}}\mathrm{e}^{-x^2} = \begin{cases} \dfrac{\sigma d}{k}\sqrt{2}(1+\operatorname{erf} x) & (x < 0), \\ \dfrac{\sigma d}{k}\sqrt{2}(1+\operatorname{erf} x) & (x > 0), \end{cases}$$

where $\operatorname{erf} x$ is the error function defined by

$$\operatorname{erf} x = \frac{2}{\sqrt{\pi}}\int_0^x \mathrm{e}^{-t^2}\, \mathrm{d}t$$

and

$$x = \pm\frac{a}{\sigma\sqrt{2}}.$$

Note that values of $\operatorname{erf} x$ and $2\mathrm{e}^{-x^2}/\sqrt{\pi}$ are tabulated (see the *Handbook of Mathematical Functions*, edited by M. A. Abramowitz and I. A. Stegun, Dover Publications, 1972). Thus if $a^* < 0$ (i.e. it is best to arrive before the mean departure time) the equation

$$\frac{2}{\sqrt{\pi}}\mathrm{e}^{-x^2} = \frac{\sigma d}{k}\sqrt{2}(1+\operatorname{erf} x)$$

must be solved and the $a^* = -\sqrt{2}\sigma x$. If $a^* > 0$ (i.e. if I can afford to arrive after the mean departure time) the equation

$$\frac{2}{\sqrt{\pi}}e^{-x^2} = \frac{\sigma d}{k}\sqrt{2}(1-\operatorname{erf} x)$$

must be solved and then $a^* = \sqrt{2}\sigma x$. Approximate results are shown in table 1 for several values of the dimensionless parameter $\sigma d/k$. (Note: if a standard unit of discomfort (cost) is defined to be the discomfort (cost) suffered during an interval of length σ, then $k/\sigma d$ is simply the penalty measured in standard units.)

Table 1. Optimal arrival times for a^* for various values of $\sigma d/k$, when T has a normal distribution $N(0, \sigma^2)$

$\frac{\sigma d}{k}$	0.1	0.3	0.6	0.8	1.0
a^*	-1.69σ	-0.97σ	-0.33σ	0	$+0.30\sigma$

For example, suppose the standard deviation σ is 3 minutes and the penalty $k = 10d$, then $\sigma d/k = 0.3$ and therefore my optimal arrival time is -0.97σ, approximately 3 minutes before the mean departure time. If $\sigma = 8$ minutes and $k = 10d$ my optimal arrival time coincides with the mean departure time. For a given value of k/d, the larger the variability in bus departure time the later the optimal arrival time; for a given variability σ, the larger the penalty k the earlier the optimal arrival time.

4. Dependence of a^* on the distribution of T

Comparison of the a^* values for the different distributions of T considered above is awkward because the distributions have different means. If the distributions are translated so as to have a common mean of zero, then comparison with the results for the normal distribution $N(0, \sigma^2)$ becomes possible. The results are shown in table 2 and figure 2.

Table 2. Values of a^* for various values of $\sigma d/k$ and different distributions each with zero mean

$\frac{\sigma d}{k}$	Uniform	Exponential	Gamma $n = 2$	Gamma $n = 3$	Normal
0.1	-1.73σ	$-\sigma$	-1.36σ	-1.49σ	-1.69σ
0.3	-1.60σ	$-\sigma$	-1.22σ	-1.22σ	-0.97σ
0.6	$+0.06\sigma$	$-\sigma$	-0.89σ	-0.76σ	-0.33σ
0.8	$+0.48\sigma$	$-\sigma$	-0.40σ	-0.24σ	0
1.0	$+0.73\sigma$	†	$+0.29\sigma$	$+0.30\sigma$	$+0.30\sigma$

† Any value $\geqslant -\sigma$

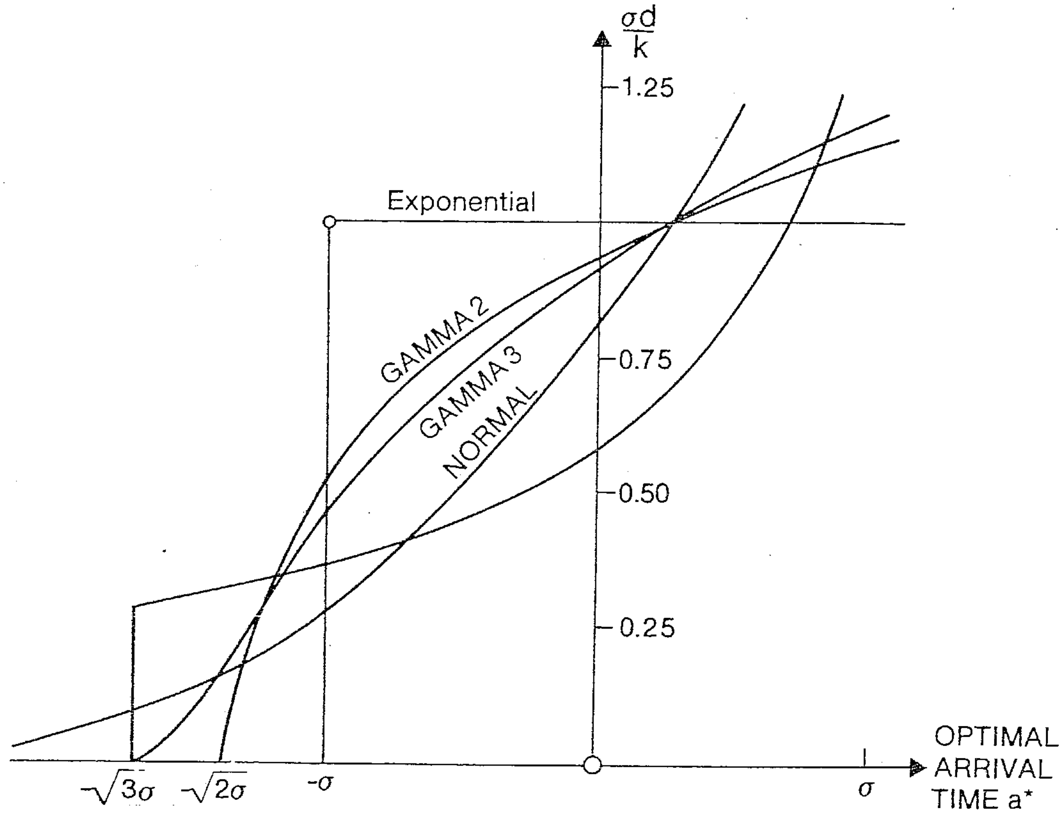


Figure 2. Values of a^* for various values of $\sigma d/k$ and different distributions each with zero mean

---

Growing Plants

A water weed grows 3 feet on the first day and its growth on each succeeding day is half that on the preceding day. A reed grows 1 foot on the first day and its growth on each succeeding day is twice that of the preceding day. When are they of equal size?

DAVID SINGMASTER
Polytechnic of the South Bank
(submitted on behalf of
Chiu Chang Suan Shu *ca.* 150BC)

Summation Properties of $\{1, 2, \ldots, n\}$

HARRIS SHULTZ, *California State University*

Harris Shultz is the author of 40 published articles, including two in *Mathematical Spectrum*. He has directed three National Science Foundation summer institutes for pre-college teacher enhancement, and was named 1988 Outstanding Professor at California State University, Fullerton.

'Generalization' is a recurring theme in mathematics. An interesting example often leads to a search for others (and perhaps all) which are similar to the original. For example, the identity $3^2+4^2 = 5^2$ serves to motivate the search for all Pythagorean triples. In this article we look at four interesting summation properties possessed by certain of the sets $\{1,2,\ldots,n\}$ and then, for each property, determine all such sets. We begin by noticing that the set $\{1,2,\ldots,11\}$ can be partitioned into two disjoint subsets, $\{1,2,4,7,8,11\}$ and $\{3,5,6,9,10\}$, such that the sum of the elements of the first subset equals that of the second. The generalization to which this example leads is introduced by the following question.

Question 1. For which natural numbers n can we find disjoint non-empty subsets A and B such that $A \cup B = \{1,2,\ldots,n\}$ and the sum of the elements of A equals that of B?

We shall call such an n a *partition number*. Observe that for n to be a partition number it is necessary that $\frac{1}{2}n(n+1)$ be even; therefore, it is necessary that either n or $n+1$ be a multiple of 4. We show that this condition is also sufficient. First note that 3 and 4 are partition numbers since $1+2 = 3$ and $1+4 = 2+3$.

Theorem. If n is a partition number then so is $n+4$.

Proof. If n is a partition number, then there exist disjoint sets A and B such that $A \cup B = \{1,2,\ldots,n\}$ and the sum of the elements of A equals that of B. Defining the disjoint sets $A' = A \cup \{n+1, n+4\}$ and $B' = B \cup \{n+2, n+3\}$ gives us

$$A' \cup B' = \{1,2,\ldots,n,n+1,n+2,n+3,n+4\}$$

and the sum of the elements of A' equals that of B'. Therefore, $n+4$ is a partition number.

It follows now by induction that the partition numbers are precisely those n for which 4 divides either n or $n+1$. Thus, the ten smallest partition numbers are 3, 4, 7, 8, 11, 12, 15, 16, 19 and 20.

One might ask whether, for a given partition number n, the subsets A and B are necessarily unique. For $n = 20$, the induction process described above yields

$$1+4+5+8+9+12+13+16+17+20$$
$$= 2+3+6+7+10+11+14+15+18+19.$$

However, we also have $1+2+\ldots+14 = 15+16+\ldots+20$. Thus, the partition is not unique. Moreover, this second partition of $\{1,2,\ldots,20\}$ leads to our next generalization.

Question 2. For which natural numbers n does there exist k such that

$$1+2+\ldots+k = (k+1)+(k+2)+\ldots+n\,?$$

Before answering question 2, we consider a closely related problem.

Question 3. For which natural numbers n does there exist k such that

$$1+2+\ldots+(k-1) = (k+1)+(k+2)+\ldots+n\,?$$

An example of such an n is the number 8, since $1+2+3+4+5 = 7+8$. The equation in question 3 can be written as

$$\tfrac{1}{2}(k-1)k = \tfrac{1}{2}n(n+1)-\tfrac{1}{2}k(k+1)$$

which simplifies to

$$\tfrac{1}{2}n(n+1) = k^2. \qquad (1)$$

Thus, the number $\frac{1}{2}n(n+1)$ is both triangular and square. Although $k = 1$, $n = 1$ satisfies (1), $n = 1$ is not an answer to question 3 since we must have $1 < k < n$. In reference 2, equation (1) is solved by defining $x = 2n+1$ and solving Pell's equation, $x^2-8k^2 = 1$; the complete answer to question 3 is the set $\{n_1, n_2, n_3, \ldots\}$, where $k_1 = 6$, $n_1 = 8$ and

$$k_{i+1} = 3k_i+2n_i+1, \qquad n_{i+1} = 4k_i+3n_i+1 \quad (i \geqslant 1).$$

(The same problem is considered in reference 1: *Editor*.)

The five smallest answers to question 3 are $n = 8$, 49, 288, 1681 and 9800 (with corresponding values $k = 6$, 35, 204, 1189 and 6930, respectively).

We now return to question 2, which can be rephrased as solving the equation

$$\tfrac{1}{2}n(n+1) = k(k+1). \qquad (2)$$

This looks somewhat similar to equation (1). In fact, if we define $r = n-k$ and $s = 2k-n$, equation (2) becomes

$$\tfrac{1}{2}s(s+1) = r^2, \tag{3}$$

which, of course, is equation (1). Since the solution to (3) in natural numbers is given by $r_1 = 1$, $s_1 = 1$ and

$$r_{i+1} = 3r_i+2s_i+1, \qquad s_{i+1} = 4r_i+3s_i+1 \quad (i \geqslant 1),$$

the answer to question 2 is the set $\{n_1, n_2, n_3, \ldots\}$, where $k_1 = 2$, $n_1 = 3$ and

$$k_{i+1} = 3k_i+2n_i+2, \qquad n_{i+1} = 4k_i+3n_i+3 \quad (i \geqslant 1).$$

The five smallest answers to question 2 are $n = 3$, 20, 119, 696 and 4059 (with corresponding values $k = 2$, 14, 84, 492 and 2870, respectively).

Questions 1 and 3 lead naturally to the following inquiry.

Question 4. For which natural numbers n can we delete from $\{1,2,\ldots,n\}$ one element in such a way that the resulting set can be partitioned into two disjoint non-empty subsets so that the sum of the elements of one subset equals that of the other?

This is readily seen to be impossible for $n = 1$, 2 and 3 and possible for $n = 4$ $(1+2 = 3)$, 5 $(1+4 = 2+3)$, 6 $(1+3+4 = 2+6)$ and 7 $(1+2+3+5 = 4+7)$. Thus, using an induction argument identical to that given in the proof of the theorem, we can conclude that the answer to question 4 is all natural numbers greater than 3.

We see then that four distinct summation questions can be asked (and answered) about the set $\{1,2,\ldots,n\}$:

1. Can we partition $\{1,2,\ldots,n\}$ into two disjoint non-empty subsets so that the sum of the elements of one subset equals that of the other?
2. Does there exist k such that $1+2+\ldots+k = (k+1)+\ldots+n$?
3. Does there exist k such that $1+2+\ldots+(k-1) = (k+1)+\ldots+n$?
4. Can we delete from $\{1,2,\ldots,n\}$ one element in such a way that the resulting set can be partitioned into two disjoint non-empty subsets so that the sum of the elements of one subset equals that of the other?

We conclude by pointing out that question 2 has medieval origins. According to legend, some labourers were hired to dig a hole 20 cubits deep. After digging 14 cubits, they tired, ceased working and asked for 14/20 of the previously agreed wage. The employer would not oblige, arguing that payment should be based on one monetary unit for the first cubit, two units for the second, three units for the third, etc. Since, as we have seen, $1+2+\ldots+14$ is half $1+2+\ldots+20$, the labourers were paid only half the previously agreed amount.

The reader might like to formulate and investigate questions related to those presented above. For example, how many different ways can we partition $\{1,2,\ldots,n\}$ into two disjoint non-empty subsets so that sum of the elements of one subset equals that of the other?

References
1. D. Averis and D. Sharpe, When squares are triangles, *Mathematical Spectrum* **13**, 80–83, (1980/81).
2. B. Leonard and H. Shultz, Triangular squares, *The Two-Year College Mathematics Journal* **10**, 169–171, (1979).

Reduction of a Non-Linear Recurrence Relation to a Linear Form

OLIVER JOHNSON, *King Edward's School, Birmingham*

The author wrote this article whilst in the fifth form.

The following problem appeared in the 1988 British Mathematical Olympiad.

The sequence $\{a_n\}$ of integers is defined by

$$-\tfrac{1}{2} < a_{n+1} - \frac{a_n^2}{a_{n-1}} \leqslant \tfrac{1}{2}$$

with $a_1 = 2$ and $a_2 = 7$. Show that a_n is odd for all values of $n \geqslant 2$.

The definition does indeed give a unique sequence because every term is an integer and there is only one integer a_n in the range $y - \frac{1}{2} < a_n \leqslant y + \frac{1}{2}$ for a given real number y. It is worthwhile attempting to see if the sequence can be defined by a linear recurrence relation. The sequence continues with $a_3 = 25$, $a_4 = 89$ and $a_5 = 317$. Now

$$\begin{aligned} a_3 &= 25 = 3\times 7 + 2\times 2 = 3a_2 + 2a_1, \\ a_4 &= 89 = 3\times 25 + 2\times 7 = 3a_3 + 2a_2, \\ a_5 &= 317 = 3\times 89 + 2\times 25 = 3a_4 + 2a_3. \end{aligned}$$

It appears that $\{a_n\}$ is identical to the sequence $\{b_n\}$ defined by

$$b_n = 3b_{n-1} + 2b_{n-2} \quad (n > 2), \qquad b_1 = 2, \qquad b_2 = 7.$$

It is clear inductively that b_n is odd whenever $n \geqslant 2$ so that, if we can prove that the two sequences are the same, this will solve the Olympiad problem.

We now prove by induction on n that

$$-\tfrac{1}{2} < b_{n+1} - \frac{b_n^2}{b_{n-1}} \leqslant \tfrac{1}{2}$$

for all $n \geqslant 2$. Since $b_3 = 25$, $b_2 = 7$ and $b_1 = 2$, the result is easily verified when $n = 2$. Now let $n > 2$ and assume that

$$-\tfrac{1}{2} < b_n - \frac{b_{n-1}^2}{b_{n-2}} \leqslant \tfrac{1}{2}.$$

Then

$$\begin{aligned} b_{n+1} - \frac{b_n^2}{b_{n-1}} &= 3b_n + 2b_{n-1} - \frac{b_n^2}{b_{n-1}} \\ &= \frac{b_n(3b_{n-1} - b_n) + 2b_{n-1}^2}{b_{n-1}} \\ &= \frac{-2b_{n-2}b_n + 2b_{n-1}^2}{b_{n-1}} \\ &= 2\left(\frac{b_{n-1}^2}{b_{n-2}} - b_n\right)\frac{b_{n-2}}{b_{n-1}} \\ &< \frac{b_{n-2}}{b_{n-1}}. \end{aligned}$$

Now, for $n > 2$, $b_n = 3b_{n-1} + 2b_{n-2} > 3b_{n-1}$, so that $b_{n-1}/b_n < \tfrac{1}{3}$. Also $b_1/b_2 = \tfrac{2}{7}$. Hence certainly

$$b_{n+1} - \frac{b_n^2}{b_{n-1}} < \tfrac{1}{2}.$$

Also,

$$b_{n+1} - \frac{b_n^2}{b_{n-1}} \geqslant -\frac{b_{n-2}}{b_{n-1}} > -\tfrac{1}{2}.$$

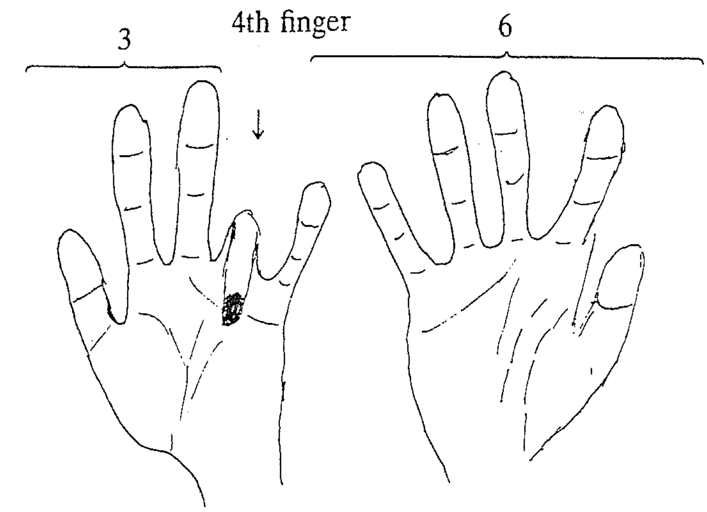
This completes the inductive step.

I have managed to generalize the problem. I have considered the sequence $\{a_n\}$ of integers defined by the same inequalities but with different starting values for a_1 and a_2, and have established that the sequence is defined by a linear recurrence relation when $a_1 = 2$ or 3, whatever the value of a_2. I have also shown that

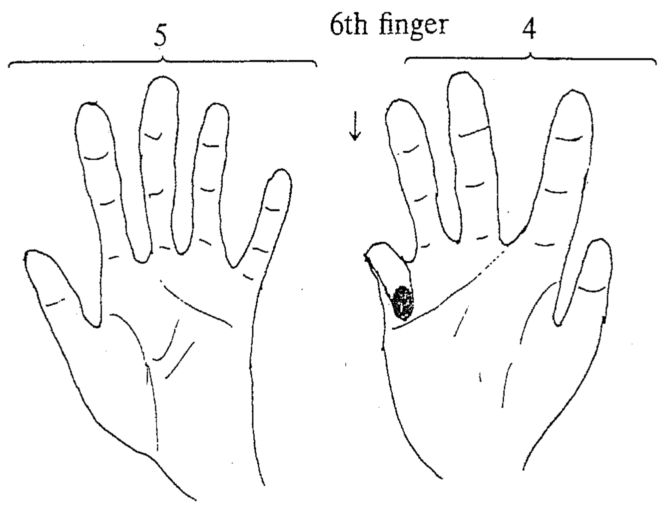
$$a_n \equiv a_{n-1} \pmod{a_1}$$

when $a_1 = 2$ and $a_2 \equiv \pm 1 \pmod 8$, and when $a_1 = 3$ and $a_2 \equiv 7$ or $14 \pmod{27}$, and a computer search indicates that this congruence holds for other starting values a_1 and a_2. Ultimately, I hope to determine for which starting values this congruence holds.

Multiplying by nine using the fingers



$4 \times 9 = 36$



$6 \times 9 = 54$

Why does it work?

ANDREW GOWAN
University of Sheffield

Error-Correcting Codes II

R. HILL, *University of Salford*

This article continues Dr Hill's account of error-correcting codes. Part I appeared in Volume 22 Number 3 of *Mathematical Spectrum*.

1. Some decimal codes and how to decode them

In this section we demonstrate the power of algebra in providing fast decoding algorithms for a large class of error-correcting codes. The codes in question are Reed–Solomon codes (the type used in compact disc players). In order to keep things simple we shall not define such codes in general but shall look at a few particular examples. We shall also restrict our attention to decimal codes, i.e. those over the alphabet $\{0, 1, \ldots, 9\}$, so that the codes are suitable for use in practical situations such as the allocation of telephone numbers or registration numbers.

To construct and implement the codes it will be necessary to carry out arithmetic (addition, subtraction, multiplication and division) with the symbols of the code alphabet. In other words, we wish the symbols of the alphabet to belong to a 'finite field'. As was mentioned in the first article (section 3.4), there exists a field of q elements if and only if q is a power of a prime number. The field of q elements is called the *Galois field of order* q and denoted by GF(q). When p is a prime number, the field GF(p) is just the set of symbols $\{0, 1, \ldots, p-1\}$ with arithmetic carried out *modulo* p. For the reader who is not familiar with modular arithmetic, let us explain what we mean by this.

Let p be a fixed positive integer. Two integers are said to be congruent (modulo p), symbolized by

$$a \equiv b \pmod{p},$$

if $a-b$ is divisible by p. Every integer n is congruent (modulo p) to a unique element in the set $\{0, 1, \ldots, p-1\}$. This unique element is just the principal remainder when n is divided by p. For example, $30 \equiv 0 \pmod{10}$, $-16 \equiv 4 \pmod{10}$, $35 \equiv 2 \pmod{11}$ and $-6 \equiv 5 \pmod{11}$.

We can now define addition, subtraction and multiplication within the set $\{0, 1, \ldots, p-1\}$ in a straightforward way. We just carry out the usual arithmetical operation and then reduce the answer modulo p (i.e. divide the answer by p to find the least non-negative remainder). Thus, in GF(11), we have

$$3+8 = 0, \qquad 6+8+10 = 2, \qquad 5-7 = 9, \qquad 6\times 5 = 8, \qquad 5^3 = 4.$$

To define division in a field, we make use of the property of a field that every non-zero element has a multiplicative inverse, i.e. given a non-zero element x there exists a unique element x^{-1} such that $xx^{-1} = 1$. When p is prime, each non-zero element $1, 2, \ldots, p-1$ has a multiplicative inverse modulo p. For example, it is readily checked that the following is a table of multiplicative inverses modulo 11:

x	1	2	3	4	5	6	7	8	9	10
x^{-1}	1	6	4	3	9	2	8	7	5	10

Division in a field is now straightforward: by a/b we just mean $a \times b^{-1}$. For example, in GF(11),

$$5/8 = 5\times 8^{-1} = 5\times 7 = 35 = 2.$$

(If p is not a prime number, then division modulo p is not possible. For example, we cannot divide by 2 (modulo 10) because 2 has no multiplicative inverse; there is no element y such that $2\times y \equiv 1 \pmod{10}$.) Finally, we mention an important further property of a field, that there are no zero divisors, i.e. we cannot have $ab = 0$ with a and b both non-zero. (If we could have $ab = 0$ with $a \neq 0$ and $b \neq 0$, then we should have $a = a(bb^{-1}) = (ab)b^{-1} = 0b^{-1} = 0$, a contradiction.)

We are now ready to describe our codes. They will be *decimal* codes, over the alphabet $\{0, 1, \ldots, 9\}$, but (since this alphabet is not itself a field) we shall regard these symbols as elements of the field GF(11). Our first example is a code in everyday use.

Example 1 (ISBN code). Every recent book has a 10-digit codeword called its International Standard Book Number (ISBN). For example, a book might have the ISBN

0-19-859617-0

although the hyphens may appear in different places (they may be ignored as far as the code is concerned). The first digit, 0, indicates the language (English) and the next two digits 19 stand for Oxford University Press, the publishers. The next six digits 859617 are the book number assigned by the publisher and the final digit is a check digit chosen to make the whole 10-digit number $x_1x_2\ldots x_{10}$ satisfy the 'check equation'

$$\sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}.$$

The ISBN code can *detect* either (a) any single error or (b) any double error created by the transposition of two digits. The error-detection scheme is simply this. For a received vector $y = y_1y_2\ldots y_{10}$, calculate $S = \sum iy_i \pmod{11}$. (S is called the *syndrome* of the received vector.) If $S = 0$ then y is a legitimate codeword and we assume there are no errors. If $S \neq 0$, then we know errors have occurred and seek retransmission. Let us verify that the scheme works for cases (a) and (b) above. Suppose $\boldsymbol{x} = x_1x_2\ldots x_{10}$ is the codeword sent.

(a) Suppose the received vector $\boldsymbol{y}$ is the same as $\boldsymbol{x}$ except that the jth symbol has an error magnitude of m. So $y_j = x_j+m$ (and $y_i = x_i$ for $i \neq j$). Then

$$S = \sum_{i=1}^{10} iy_i = \sum_{i=1}^{10} ix_i + jm = jm \neq 0$$

since j and m are non-zero (all arithmetic is carried out in GF(11)).

(b) Suppose $\boldsymbol{y}$ is the same as $\boldsymbol{x}$ except that digits x_j and x_k have been transposed. Then

$$S = \sum_{i=1}^{10} iy_i = \sum_{i=1}^{10} ix_i + (k-j)x_j+(j-k)x_k = (k-j)(x_j-x_k) \neq 0,$$

if $k \neq j$ and $x_j \neq x_k$.

Note how crucial use is made of the fact that, in a field, the product of two non-zero elements is also non-zero. It is left as an exercise for the reader to show that, if we define a code to have a check equation modulo 10 (i.e. if the code is the set of n-digit numbers $x_1x_2\ldots x_n$ satisfying a check equation of the form

$$a_1x_1+a_2x_2+\ldots+a_nx_n \equiv 0 \pmod{10}$$

for some fixed integers $a_1, a_2, \ldots, a_n$ $(n \geqslant 3)$), then we cannot detect all single errors and all transpositions.

The ISBN code cannot be used to *correct* an error unless we also know the location of the error. This is the basis of the following party trick.

Ask a friend to choose a book not known to you and to read out its ISBN, but saying 'x' for one of the digits. After a few seconds working you announce the value of x. For example, if the number read out is 0-201-1x502-7, your working is:

$$(1\times0)+(2\times2)+(3\times0)+(4\times1)+(5\times1)$$
$$+(6\times x)+(7\times5)+(8\times0)+(9\times2)+(10\times7) = 0.$$

Hence $6x+4 = 0$, and so $x = -4/6 = 7\times6^{-1} = 7\times2 = 14 = 3$.

Example 2 (a possible telephone number code). Let C be the code of all 10-digit decimal numbers $x_1x_2\ldots x_{10}$ simultaneously satisfying the two check equations

$$\sum_{i=1}^{10} x_i \equiv 0 \pmod{11}, \qquad \sum_{i=1}^{10} ix_i \equiv 0 \pmod{11}.$$

There are over 82 million such numbers (certainly enough for all the telephones in the UK).

This code is a single-error correcting code which can at the same time detect any double error caused by the transposition of two digits. The decoding scheme is as follows.

Suppose $x = x_1x_2 \ldots x_{10}$ is the codeword (unknown to us) which was transmitted and that $y = y_1y_2 \ldots y_{10}$ is the received vector. We calculate the *syndrome* (S_1, S_2) of the received vector, defined by $S_1 = \sum y_i$ and $S_2 = \sum iy_i$ (again, all arithmetic is carried out in GF(11)).

(a) If $S_1 = S_2 = 0$, the received vector is a legitimate codeword and we assume no errors.

(b) Now suppose one error has occurred of magnitude m in position j. Then we have

$$S_1 = \sum_{i=1}^{10} y_i = \sum_{i=1}^{10} x_j + m = m$$

and

$$S_2 = \sum_{i=1}^{10} iy_i = \sum_{i=1}^{10} ix_i + jm = jm.$$

Since $m \neq 0$ and $j \neq 0$ we have $S_1 \neq 0$ and $S_2 \neq 0$. So, if we find that $S_1 \neq 0$ and $S_2 \neq 0$, we assume there is a single error and solve the equations

$$m = S_1, \qquad jm = S_2$$

for m and j. Thus we have $m = S_1$ and $j = S_2/S_1$ and the error may be corrected. (In the context of telephone calls, the desired number would automatically ring out.)

(c) If $S_1 = 0$ or $S_2 = 0$ but not both, then at least two errors must have occurred and we seek retransmission. (In the telephone application a 'number unobtainable' signal would be obtained.) Case (c) must occur if two digits have been transposed, for then $S_1 = 0$ and (as for the ISBN code) $S_2 \neq 0$.

For example, suppose $y = 061\,027\,1355$. We calculate that $S_1 = 8$ and $S_2 = 6$. Hence $S_2/S_1 = 6 \times 8^{-1} = 9$ and so the 9th digit should have been $5 - 8 = -3 = 8$.

Note how much faster is this decoding scheme than the brute-force scheme of comparing the received vector with all codewords. Also, there is no need to store a list of codewords in the memory of the decoder.

Example 3 (a double-error correcting code). Let C be the code of all 10-digit numbers over GF(11) which satisfy the four check equations

$$\sum x_i = \sum ix_i = \sum i^2x_i = \sum i^3x_i = 0.$$

We now show that C is a double-error correcting code. From a received vector $y_1y_2\ldots y_{10}$ we calculate the syndrome

$$(S_1, S_2, S_3, S_4) = (\sum y_i, \sum iy_i, \sum i^2y_i, \sum i^3y_i).$$

Suppose errors of magnitude m_1 and m_2 have occurred in positions p_1 and p_2 respectively. To decode, we need to solve the four equations

$$\begin{aligned} m_1 \quad + m_2 \quad &= S_1 & (1)\\ m_1p_1 + m_2p_2 &= S_2 & (2)\\ m_1p_1^2 + m_2p_2^2 &= S_3 & (3)\\ m_1p_1^3 + m_2p_2^3 &= S_4 & (4) \end{aligned}$$

for the four unknowns m_1, m_2, p_1 and p_2. At first sight this looks rather difficult as the equations are non-linear. However, we can eliminate m_1, m_2 and p_2 as follows:

$$\begin{aligned} p_1\times(1)-(2) \quad &\text{gives} \quad m_2(p_1-p_2) = p_1S_1-S_2, & (5)\\ p_1\times(2)-(3) \quad &\text{gives} \quad m_2p_2(p_1-p_2) = p_1S_2-S_3, & (6)\\ p_1\times(3)-(4) \quad &\text{gives} \quad m_2p_2^2(p_1-p_2) = p_1S_3-S_4. & (7) \end{aligned}$$

Comparing $(6)^2$ with $(5)\times(7)$ now gives

$$(p_1S_2-S_3)^2 = (p_1S_1-S_2)(p_1S_3-S_4)$$

and so p_1 satisfies the quadratic equation

$$(S_2^2-S_1S_3)p^2+(S_1S_4-S_2S_3)p+S_3^2-S_2S_4 = 0. \qquad (8)$$

Eliminating m_1, m_2 and p_1 from (1) to (4) in similar fashion shows that p_2 also satisfies equation (8). So, from the syndrome, we can obtain the error locations p_1 and p_2 as the roots of the quadratic equation (8). Once p_1 and p_2 are found the values of m_1 and m_2 are easily obtained from (1) and (2). (Note that if just one error occurs then equations (1) to (4) have $m_1 \neq 0$ and $m_2 = 0$. This means that the coefficients of p^2 and p in equation (8) are zero and so in that event we assume a single error of magnitude S_1 in position S_2/S_1.)

Example 4 (t-error correcting codes). The single- and double-error correcting codes of Examples 2 and 3 generalize to t-error correcting codes in a natural way. Let q be a prime number and let C be the code consisting of all n-tuples $x_1x_2\ldots x_n$, with entries in GF(q), satisfying the $2t$ check equations

$$\sum_{i=1}^{n} i^{k-1}x_i = 0 \quad \text{for } k = 1,2,\ldots,2t.$$

(It is necessary to assume that $2t+1 \leqslant n \leqslant q-1$.) As usual, from a received vector $y_1y_2\ldots y_n$, we calculate the syndrome $(S_1, S_2, \ldots, S_{2t})$, where

$$S_k = \sum_{i=1}^{10} i^{k-1}y_i.$$

Assuming that errors of magnitude $m_1, m_2, \ldots, m_t$ have occurred in positions $p_1, p_2, \ldots, p_t$, respectively, then to decode we must solve, for the m_i's and p_i's, the following system of equations:

$$\begin{array}{lllll}
m_1 & +m_2 & +\ldots & +m_t & = S_1 \\
m_1p_1 & +m_2p_2 & +\ldots & +m_tp_t & = S_2 \\
m_1p_1^2 & +m_2p_2^2 & +\ldots & +m_tp_t^2 & = S_3 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
m_1p_1^{2t-1} & +m_2p_2^{2t-1} & +\ldots & +m_tp_t^{2t-1} & = S_{2t}
\end{array}$$

For $t \geqslant 3$, the equations are too complicated to eliminate $2t-1$ unknowns as we did for the case $t = 2$. (The case $t = 3$ was considered in a recent *Spectrum* article (reference 1) by Dermot Roaf, who gave three elegant methods of solution.)

In the early 1960s coding theorists devised neat methods of solving such systems. They were unaware of the fact that, fifty years previously, a method of solving precisely such a system had been given by the famous self-taught Indian mathematician Srinivasa Ramanujan. Ramanujan's method of solution may be found in reference 2 or in Chapter 11 of reference 3. Astonishingly, as was pointed out by J. K. Wolf in reference 4, the solving of such systems of equations has a much older history—it dates back to a French theoretical engineer named R. Prony in 1795! How and why Prony did it is the topic of our final section.

2. Prony's method and the debt to Lagrange

At first sight, it seems remarkable that the elegant and by no means obvious method of solution used by Ramanujan could have been found previously as long ago as 1795. But on reading Prony's original paper (reference 5, in French of course), one finds that his solution arises quite naturally out of the context in which he was studying the equations. This is in contrast to Ramanujan's solution, which, although essentially the same, gives the impression of having being 'pulled out of a hat'. It is interesting to see also how Prony makes use of two quite different areas of now familiar mathematics which at that time had only just been developed by the great French mathematician, Joseph-Louis Lagrange (1736–1813).

Prony, or to give him his full name, Gaspard Riche, baron de Prony, was born in 1755. He originally trained in classics and did not study mathematics seriously until the age of 20. He graduated in mathematics at the age of 25 and went on to become France's leading engineer and engineering educator until his death in 1839. He greatly influenced the course of civil engineering in France and was instrumental in the construction of numerous bridges. He was also put in charge of a project to produce tables of trigonometric functions to 14 decimal places and achieved this by allocating the work among several hundred men who knew only the elementary rules of arithmetic (one of the earliest examples of parallel processing?). Napoleon made him a member of the Legion of Honour on its foundation.

Let us now see how it came about that Prony needed to solve a certain system of equations. In the early 1790s, Prony was seeking formulae to describe various physical phenomena, such as properties of gases as functions of temperature. The problem Prony faced was this. From experiments he knew the values of a function $f(x)$ at $2n$ equally spaced values of x. By suitable scaling, one may assume that these x-values are $0, 1, \ldots, 2n-1$. Prony's problem was one of curve-fitting; which function $f(x)$ passes through the known values $f(0), f(1), \ldots, f(2n-1)$? What type of function might be tried? Prony knew from experience that the functions he was interested in could often be approximated either by a geometric progression or by a sum of geometric progressions. He therefore considered seeking a function of the form

$$f(x) = \mu_1\rho_1^x + \mu_2\rho_2^x + \ldots + \mu_n\rho_n^x, \tag{1}$$

where the μ_i's and ρ_i's were constants to be determined. He thus had $2n$ unknowns to be determined from the $2n$ equations:

$$\begin{array}{llllll} \mu_1 & +\mu_2 & + \ldots & +\mu_n & = f(0) \\ \mu_1\rho_1 & +\mu_2\rho_2 & + \ldots & +\mu_n\rho_n & = f(1) \\ \mu_1\rho_1^2 & +\mu_2\rho_2^2 & + \ldots & +\mu_n\rho_n^2 & = f(2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \mu_1\rho_1^{2n-1} & +\mu_2\rho_2^{2n-1} & + \ldots & +\mu_n\rho_n^{2n-1} & = f(2n-1) \end{array} \tag{2}$$

This is precisely the system of equations involved in the decoding of the Reed–Solomon codes of Example 4. The only difference is that in the curve-fitting problem one works with the field of real (or complex) numbers, while in the coding problem one is concerned with a finite field. The methods of solution, however, are identical.

The key step in Prony's method of solution was his observation that the function $f(x)$ given by (1) arises as the solution of a constant-coefficient linear difference equation of order n. In other words, $f(x)$ will have the form of (1) if, for each integer $m \geqslant n$, $f(m)$ is the same linear combination of the values of f at the preceding n points; that is, $f(m)$ satisfies a recurrence relation

$$f(m)+a_{n-1}f(m-1)+\ldots+a_1f(m-n+1)+a_0f(m-n) = 0 \tag{3}$$

for some constants $a_0, a_1, \ldots, a_{n-1}$.

Prony was able to make this observation because, only a few years earlier, Lagrange had published the first complete algebraic theory of recurring series with constant coefficients. (Lagrange's work generalized the earlier work of A. de Moivre who in 1718 had solved the most famous recurrence relation of all—he had found an explicit formula for the Fibonacci numbers, which are defined by the recurrence relation $f(m) = f(m-1)+f(m-2)$ with $f(0) = f(1) = 1$.)

As readers who are familiar with difference equations will know, to solve a relation of type (3), one considers a trial solution of the form $f(m) = \rho^m$. Substitution into (3) gives

$$\rho^m+a_{n-1}\rho^{m-1}+\ldots+a_0\rho^{m-n} = 0,$$

and so, assuming $\rho \neq 0$ and cancelling by ρ^{m-n}, we find that ρ satisfies the polynomial equation

$$x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0 = 0. \tag{4}$$

Equation (4) is called the characteristic equation of the difference equation (3). If (4) has roots $\rho_1, \rho_2, \ldots, \rho_n$, then the function

$$f(m) = \mu_1\rho_1^m+\mu_2\rho_2^m+\ldots+\mu_n\rho_n^m$$

is a solution of (3) for constants $\mu_1, \mu_2, \ldots, \mu_n$, which may be determined from the initial values $f(0), f(1), \ldots, f(n-1)$.

Returning to Prony's method, we do not yet know what the coefficients of the difference equation (3) are; all we know initially are the values $f(0), f(1), \ldots, f(2n-1)$. But from these values and relation (3), we get the following system of n simultaneous linear equations in the n unknowns $a_0, a_1, \ldots, a_{n-1}$:

$$\begin{array}{llllll} f(n) & +a_{n-1}f(n-1) & +\ \ldots & +a_1f(1) & +a_0f(0) & = 0 \\ f(n+1) & +a_{n-1}f(n) & +\ \ldots & +a_1f(2) & +a_0f(1) & = 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ f(2n-1) & +a_{n-1}f(2n-2) & +\ \ldots & +a_1f(n) & +a_0f(n-1) & = 0 \end{array} \tag{5}$$

So the a_i's may be found by solving the system (5), and then $\rho_1, \rho_2, \ldots, \rho_n$ found as the roots of (4). Once the ρ_i's are known, one can find the μ_i's simply by solving the linear system in the μ_i's given by the first n equations of (2). This completes Prony's method.

But is the above procedure quite so straightforward as it seems? One of the steps was to find the roots of the polynomial equation (4) of degree n. It was shown by Galois in 1832 that there is no general formula (such as the familiar one by which the roots of a quadratic may be found) for finding the roots of a general quintic polynomial equation (i.e. one of degree 5). For coding theorists, finding the roots of (4) presents no problem because all the numbers involved belong to a *finite* field and so the roots may be found by trial substitution of all the field elements. Ramanujan, working over the field of reals, did not discuss the difficulty. He gave an example of his method (taking $n = 5$ and $f(0), f(1), \ldots, f(9)$ to be 2, 3, 16, 31, 103, 235, 674, 1669, 4526 and 11595 respectively in which equation (4) turns out to be the quintic

$$x^5 - x^4 - 5x^3 + x^2 + 3x - 1 = 0.$$

This fortuitously factorized into $(x+1)(x^2-3x+1)(x^2+x-1) = 0$ to give the roots -1, $\frac{1}{2}(3 \pm \sqrt{5})$ and $\frac{1}{2}(-1 \pm \sqrt{5})$. One rather suspects that Ramanujan worked back from an answer in order to pose his problem!

But what was Prony to do back in 1795 to find the roots of equation (4), bearing in mind that in his applications the a_i's would be rather unpleasant numbers given to several decimal places? Again, Lagrange had provided the answer. In 1767 in his work 'On the solution of numerical equations', Lagrange had, for the first time, provided a method of solving equations such as (4) numerically to a preassigned degree of accuracy.

In view of the reliance of Prony's method on Lagrange's work, it seems fitting that Prony's paper was published in Volume 1 of the *Journal de l'École Polytechnique*; the famous École had just been founded—with Lagrange as its first professor of mathematics!

References

1. D. Roaf, Ramanujan's third problem, *Mathematical Spectrum* **21** (1988/89), 73–78.

2. S. Ramanujan, Note on a set of simultaneous equations, *Journal of the Indian Mathematical Society* **4** (1912), 94–96.

3. R. Hill, *A First Course in Coding Theory* (Oxford University Press, 1986).

4. J. K. Wolf, Decoding of Bose–Chaudhuri–Hocquengham codes and Prony's method for curve fitting, *IEEE Transactions on Information Theory* **13** (1967), 608.

5. R. de Prony, Essai experimentale et analytique, *Journal de l'École Polytechnique (Paris)* **1** (1795), 24–76.

Polynomials with Prime Values

M. G. VERTANNES

The author is a student with the Open University and lives in Swindon.

In 1772, Euler discovered the formula $f(n) = n^2+n+41$ which gives prime values for $n = 0, 1, 2, \ldots, 39$, although it is clearly divisible by 41 when $n = 40$. The prime numbers produced by $n = 0, 1, \ldots, 39$ are given below.

41	43	47	53	61	71	83	97	113	131
151	173	197	223	251	281	313	347	383	421
461	503	547	593	641	691	743	797	853	911
971	1033	1097	1163	1231	1301	1373	1447	1523	1601

Note that $f(-1-n) = f(n)$, so that

$$f(-1) = f(0), \qquad f(-2) = f(1), \qquad \ldots, \qquad f(-40) = f(39).$$

In 1899, E. B. Escott gave the formula $n^2-79n+1601$, which gives the same prime numbers for $n = 0$ to 79, each repeated twice, but fails to be prime when $n = 80$. In fact, this formula is just $f(n-40)$, which explains why the same primes appear and appear twice.

We can fill in the gap between Euler's formula and Escott's if we consider $f(n-k)$ for $k = 1$ to 39. This will take the same prime values as Euler's formula for $n = 0$ to $39+k$ with the first k values occurring twice.

It is known that there is no polynomial with integer coefficients which takes prime values for all integer values of its variable (see the reference, theorem 21). Euler's formula n^2+n+41 is prime for 581 values of n in the range $0 \leqslant n \leqslant 1000$. However, $2n^2-199$ takes slightly more prime values in this range. Surprisingly, there do not appear to be any results giving a polynomial in n which takes more than 40 distinct prime values for consecutive values of n.

Reference

G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edn (Clarendon Press, Oxford, 1979).

Evaluate the expression

$$(m-a)(m-b)(m-c)\ldots(m-x)(m-y)(m-z).$$

VICTOR NICOLA
South Bank Polytechnic

Computer Column

MIKE PIFF

Generating subsets

We all know that if a set has n elements then the number of its subsets equals 2^n. Sometimes, it is necessary to search through all these subsets, and to do a calculation on each one. Thus, we need a procedure to generate these subsets one after another, to make sure we have considered them all.

The program in this issue contains such a procedure. It takes a set as an argument, and changes that set to the 'next' set, according to its own idea of what order subsets should be in.

A set is stored in this implementation as a record, which consists of a boolean array indexed by the elements, and also the number of elements in the set we are considering. This record type allows us to declare variables that are sets, and to operate on those sets. Thus, as an exercise, try writing procedures to take unions and intersections of sets, declared by

```
PROCEDURE Union(s1,s2 : sets; VAR s1unions2 : sets);
```

say.

```
MODULE Subsets;
FROM InOut IMPORT ReadCard,WriteCard,WriteLn,
WriteString,Write;
CONST
  minelt=1; maxelt=100; bset='{'; eset='}';
TYPE
  elts=CARDINAL[minelt..maxelt];
  membership=ARRAY elts OF BOOLEAN;
  sets=RECORD
    nrfelts:elts;
    member:membership;
  END;
VAR
  s:sets;
  empty:BOOLEAN;
PROCEDURE Initialise(VAR s:sets);
VAR
  i:elts;
  j:CARDINAL;
BEGIN
  WITH s DO
    WriteString('Give number of elements ');
    ReadCard(j);nrfelts:=elts(j);WriteLn;
    FOR i:=minelt TO nrfelts DO
      member[i]:=FALSE;
    END;
  END;
END Initialise;
PROCEDURE NextSet(VAR s:sets;VAR empty:BOOLEAN);
VAR
  i:[minelt..maxelt+1];
  done:BOOLEAN;
BEGIN
  i:=minelt; done:=FALSE;
  WITH s DO
    REPEAT
      IF member[i] THEN
        member[i]:=FALSE; INC(i);
      ELSE
        done:=TRUE; member[i]:=TRUE;
      END;
    UNTIL done OR (i>nrfelts);
    empty:=~done;
  END;
END NextSet;
PROCEDURE WriteSet(VAR s:sets);
VAR
  i:elts;
BEGIN
  WITH s DO
    Write(bset);
    FOR i:=minelt TO nrfelts DO
      IF member[i] THEN
        WriteCard(i,3);
      END;
    END;
    Write(eset);
  END;
  WriteLn;
END WriteSet;
BEGIN
  Initialise(s);
  REPEAT
    NextSet(s,empty); WriteSet(s);
  UNTIL empty;
END Subsets.
```

Letters to the Editor

Dear Editor,

Ramanujan's approximation to $2^{1/3}$

One of the advantages of advancing technology is the ability to investigate, quickly and easily, questions that earlier would have been, if not intractable, at least of insufficient interest to warrant the time required. Out of curiosity, I used Mathematica™ to play with the formulae given in D. Somasundaram's 'Some Fascinating Formulae of Ramanujan' (*Mathematical Spectrum* Volume 20, Number 3, page 85). I noticed that the approximation to $2^{1/3}$ attributed to Ramanujan is in error after the 21st decimal digit; where '208' is given, '211' actually occurs (which is rounded from '2106').

Yours sincerely,

BARRY W. BRUNSON
(Department of Mathematics,
Western Kentucky University,
Bowling Green, KY 42101, USA)

Dear Editor,

A factorial identity from difference tables

On reading the second chapter of the excellent *Concrete Mathematics* (reference 1), my mind was cast back to a problem posed in the Letters to the Editor section of Volume 21 Number 2:

Show that

$$n! = A^n - \binom{n}{1}(A-1)^n + \binom{n}{2}(A-2)^n - \ldots + (-1)^n(A-n)^n, \tag{1}$$

where n is a positive integer and A is real.

I propose a more direct proof than that given in the Solutions to Problems of Volume 22 Number 2.

We start by restating the problem from which this was derived: What is the constant in the $(n+1)$th row of the difference table whose first row is $A^n, (A+1)^n, (A+2)^n, \ldots$, where A is real?

First some useful definitions from *Concrete Mathematics*:

$$\binom{x}{k} = x(x-1)(x-2)\ldots(x-k+1), \qquad \binom{x}{0} = 1, \qquad \Delta(f(x)) = f(x+1) - f(x).$$

So we have

$$\Delta(g+h) = \Delta(g) + \Delta(h), \qquad \Delta\binom{x}{k} = k\binom{x}{k-1}.$$

(These are curiously analogous to continuous calculus.)

By induction on k, x^k can always be expressed in the form

$$\binom{x}{k}+a_{k-1}\binom{x}{k-1}+a_{k-2}\binom{x}{k-2}+\ldots+a_1\binom{x}{1}.$$

Finding a function for the $(n+1)$th row of the difference table is equivalent to applying Δ n times to x^n:

$$\Delta^n(x^n) = \Delta^n\left\{\binom{x}{n}+a_{n-1}\binom{x}{n-1}+\ldots+a_1\binom{x}{1}\right\} = n!.$$

Now, by induction,

$$\Delta^n(f(x)) = \sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}f(x+k),$$

and (1) follows.

Reference

1. R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics, a Foundation for Computer Science* (Addison Wesley, Reading, MA, 1989).

Yours sincerely,

DYLAN GOW
(Y6 Angel Court,
Trinity College, Cambridge)

Problems and Solutions

Sixth formers and students are invited to submit solutions to some or all of the problems below: the most attractive solutions will be published in subsequent issues. When writing to the Editorial Office, please state your full name and also the postal address of your school, college or university.

Problems

23.1 (Submitted by Amites Sarkar, Winchester College)
Denote by O the centroid of a regular icosahedron with vertices $A_1, A_2, \ldots, A_{12}$, labelled so that $|A_1A_i| \leqslant |A_1A_j|$ for $i<j$. Determine the angle A_1OA_2.

23.2 (Submitted by Gregory Economides, University of Newcastle upon Tyne)
Find the sum of the series

$$\sum_{r=1}^{n}\frac{1}{\sin 2^r x},$$

where x is a real number and $2^r x$ is not an integer multiple of π for $r=0,1,\ldots,n$.

23.3 (Submitted by P. Glaister, University of Reading)
Let PQ be an arc of a circle, centre O, with angle $POQ < 90°$, and denote by R the foot of the perpendicular from Q to OP. Show that the volume of the cone obtained by rotating OQR through 360° about OR is equal to the volume of the solid obtained by rotating RQP through 360° about RP if and only if R divides OP in the golden ratio.

Solutions to Problems in Volume 22 Number 2

22.5. The methane molecule is based on a regular tetrahedron with the carbon atom at the centroid and the four hydrogen atoms at the vertices. What is the angle between pairs of carbon valency links—all to hydrogen?

Solution 1 by Dylan Gow (Trinity College, Cambridge)

Let $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ and $\boldsymbol{d}$ denote the position vectors of the hydrogen atoms with respect to the carbon atom as origin, all of unit length. Then

$$\boldsymbol{a}\cdot\boldsymbol{b} = \boldsymbol{a}\cdot\boldsymbol{c} = \boldsymbol{a}\cdot\boldsymbol{d} = \boldsymbol{b}\cdot\boldsymbol{c} = \boldsymbol{b}\cdot\boldsymbol{d} = \boldsymbol{c}\cdot\boldsymbol{d} = \cos\theta,$$

where θ is the angle between bonds. By symmetry,

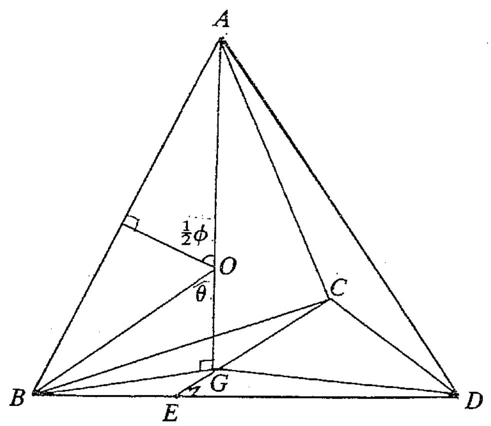
$$\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}+\boldsymbol{d} = \boldsymbol{0},$$

so that

$$\begin{aligned}
& (\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}+\boldsymbol{d})\cdot(\boldsymbol{a}+\boldsymbol{b}+\boldsymbol{c}+\boldsymbol{d}) = 0 \\
\Rightarrow\quad & 4+2(\boldsymbol{a}\cdot\boldsymbol{b}+\boldsymbol{a}\cdot\boldsymbol{c}+\boldsymbol{a}\cdot\boldsymbol{d}+\boldsymbol{b}\cdot\boldsymbol{c}+\boldsymbol{b}\cdot\boldsymbol{d}+\boldsymbol{c}\cdot\boldsymbol{d}) = 0 \\
\Rightarrow\quad & 4+12\cos\theta = 0 \\
\Rightarrow\quad & \cos\theta = -\tfrac{1}{3},
\end{aligned}$$

so that θ is approximately $109°28'$.

Solution 2 by Amites Sarkar



$ABCD$ is a regular tetrahedron with $AB = 1$ and centroid O. The centroid of triangle BCD is G, $OA = a$, $\angle AOB = \phi$, $\angle BOG = \theta$, E is on BD with $BE = ED$ and $\theta+\phi = \pi$, so that $\sin\theta = \sin\phi$. Now $\angle GBE = \frac{1}{6}\pi$, so that $GE = \frac{1}{2}BG = \frac{1}{2}CG$ and $CG = \frac{2}{3}CE = 1/\sqrt{3}$. Therefore $\sin\phi = \sin\theta = 1/\sqrt{3}a$ and $\sin\frac{1}{2}\phi = 1/2a$. This gives

$$2\cos\tfrac{1}{2}\phi = \frac{\sin\phi}{\sin\frac{1}{2}\phi} = \frac{2}{\sqrt{3}} \Rightarrow \cos\tfrac{1}{2}\phi = \frac{1}{\sqrt{3}},$$

so that

$$\phi = 2\cos^{-1}\left(\frac{1}{\sqrt{3}}\right) = \cos^{-1}(-\tfrac{1}{3}).$$

22.6. How many non-similar integer-angled triangles are there (the angles being measured in degrees)?

Solution by Amites Sarkar

The number of integer-angled triangles with smallest angle $n°$ is

$$\tfrac{1}{2}(180-n)-n+1 = 91-\tfrac{3}{2}n \quad \text{or} \quad \tfrac{1}{2}(180-n)-\tfrac{1}{2}-n+1 = \tfrac{181}{2}-\tfrac{3}{2}n$$

according as n is even or odd. (For example, if $n = 20$ the triangles have angles $(20°, 20°, 140°)$, $(20°, 21°, 139°)$, $\ldots$, $(20°, 80°, 80°)$; if $n = 21$, they have angles $(21°, 21°, 138°)$, $(21°, 22°, 137°)$, $\ldots$, $(21°, 79°, 80°)$.) Therefore the total number of integer-angled triangles is

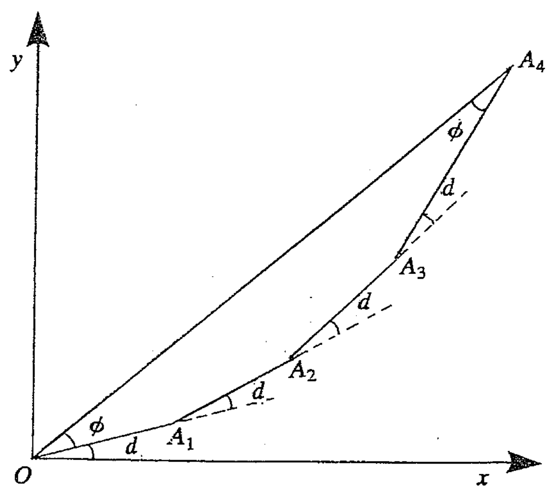
$$\begin{aligned}\sum_{k=1}^{30}\{[91-\tfrac{3}{2}(2k)]+[\tfrac{181}{2}-\tfrac{3}{2}(2k-1)]\} &= \sum_{k=1}^{30}(183-6k)\\ &= 30\times183-6\times\tfrac{1}{2}\times30\times31\\ &= 2700.\end{aligned}$$

Also solved by Dylan Gow.

22.7. Show that

$$\frac{\sum_{r=0}^{n-1}\sin(rd+a)}{\sum_{r=0}^{n-1}\cos(rd+a)} = \tan\{\tfrac{1}{2}(n-1)\,d+a\}.$$

Solution by Dylan Gow, who submitted the problem.



The figure illustrates the case $n = 4$. The line segment OA_1 is of length l at an angle a with the x-axis, A_1A_2 is of length l at an angle d with OA_1, and so on to $A_{n-1}A_n$. A complete revolution is given by

$$(n-1)\,d+(\pi-\phi)+(\pi-\phi) = 2\pi,$$

so that $\phi = \frac{1}{2}(n-1)\,d$. The coordinates of A_n are

$$\left(\sum_{r=0}^{n-1}\cos(a+rd),\ \sum_{r=0}^{n-1}\sin(a+rd)\right),$$

so that

$$\frac{\sum_{r=0}^{n-1}\sin(a+rd)}{\sum_{r=0}^{n-1}\cos(a+rd)} = \tan(a+\phi) = \tan\{a+\tfrac{1}{2}(n-1)\,d\}.$$

Also solved by Amites Sarkar.

22.8. The sequence (A_r) is defined as follows:

$$A_1 = A_2 = A_3 = 1, \qquad A_{r+1} = A_{r-1}+A_{r-2} \quad (r > 2).$$

Prove the identity $A_{2n} = 2A_nA_{n-1}+A_{n-2}^2$ for $n > 2$.

Solution by Dylan Gow

Define the matrix M by

$$M = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Now

$$M\begin{bmatrix} A_{n-1} & A_n & A_{n-2} \\ A_{n-2} & A_{n-1} & A_{n-3} \\ A_{n-3} & A_{n-2} & A_{n-4} \end{bmatrix} = \begin{bmatrix} A_n & A_{n+1} & A_{n-1} \\ A_{n-1} & A_n & A_{n-2} \\ A_{n-2} & A_{n-1} & A_{n-3} \end{bmatrix}.$$

We can extend the sequence by writing $A_0 = 0$, $A_{-1} = 1$, $A_{-2} = 0$ and $A_{-3} = 0$. Then

$$M^n = \begin{bmatrix} A_{n-1} & A_n & A_{n-2} \\ A_{n-2} & A_{n-1} & A_{n-3} \\ A_{n-3} & A_{n-2} & A_{n-4} \end{bmatrix}.$$

It follows that

$$\begin{bmatrix} A_{n-1} & A_n & A_{n-2} \\ A_{n-2} & A_{n-1} & A_{n-3} \\ A_{n-3} & A_{n-2} & A_{n-4} \end{bmatrix}^2 = M^{2n} = \begin{bmatrix} A_{2n-1} & A_{2n} & A_{2n-2} \\ A_{2n-2} & A_{2n-1} & A_{2n-3} \\ A_{2n-3} & A_{2n-2} & A_{2n-4} \end{bmatrix}.$$

We now equate (1, 2)th elements to give

$$A_{2n} = 2A_nA_{n-1} + A_{n-2}^2 \quad (n > 2).$$

Note. This solution is similar to the approach to the Fibonacci sequence given in Norman Routledge's letter in Volume 22 Number 2 page 63. Amites Sarkar, who submitted the problem, and Norman Routledge have pointed out how a further identity may be obtained. It is easy to verify directly that $M^3 = M+I$ (or use the Cayley–Hamilton theorem). Hence $M^{3n} = (M+I)^n$. If we equate (1, 2)th elements, we obtain the identity

$$A_{3n} = \binom{n}{0}A_n + \binom{n}{1}A_{n-1} + \binom{n}{n-2}A_{n-2} + \dots + \binom{n}{n-1}A_1.$$

The 1990 puzzle (page 71)

The second-year pupils at The Honywood School, Coggeshall, Essex, have been successful in expressing 86 of the integers 1 to 100 in the required form, which is a much higher success rate than we had anticipated. Why not have a go? (Don't forget that 0! = 1.)

Reviews

Let Newton Be! Edited by JOHN FAUVEL, RAYMOND FLOOD, MICHAEL SHORTLAND, and ROBIN WILSON. Clarendon Press, Oxford, 1988. Pp. 272. £17.50 (ISBN 0-19-853924-X).

This beautifully produced, copiously illustrated book is a sheer joy to browse through and would make a handsome addition to any library. Occasioned by the celebration of the 300th anniversary of the appearance of Newton's *Principia* in 1687, it draws on recent research to project a fresh view of the world's greatest scientist. *Let Newton Be!* covers an extraordinary variety of Newton's work from mathematics to theology, from mechanics to music, and from optics to alchemy. It is lucidly written by a team of experts in the history of science, and should appeal to the general reader and specialist alike.

Just flicking through the pages and studying the photographs can be an enjoyable experience in itself. A page from Newton's notebook lists some of the fifty sins that he had committed during his life up to Whit Sunday 1662; these included swimming on the Sabbath, and threatening to burn down his parents' house with them inside it. There is a delightful picture of Harpo Marx playing Newton in the 1957 film *The story of mankind*. An elaborate frontispiece to Newton's *Method of Fluxions* depicts two country gentlemen with their gun dogs out on a bird shoot, while a group of ancient Greeks look on admiringly—the whole effect being designed to show the benefit to traditional English rural pursuits of Newton's calculus because of the ease with which it could treat problems of motion!

Some chapters of the book are particularly valuable in that they discuss aspects of Newton's studies which have so far passed almost unnoticed in the literature. One such is 'The harmonic roots of Newtonian science' by Penelope Gouk. In this she suggests that a possible reason for the neglect of Newton's musical studies was his complete lack of interest in musical performance itself. For example, he 'never was at more than one Opera. The first Act he heard with pleasure, the 2nd stretch'd his patience, at the 3rd he ran away'. On another occasion 'Newton, hearing Handel play upon the harpsichord, could find nothing worthy to remark but the flexibility of his fingers'.

Oxford University Press, the editors and the authors are to be congratulated on producing this excellent new perspective on Newton. It is to be hoped that the assured success of *Let Newton Be!* will bring forth a paperback edition, so enabling it to reach the wider readership that it so justly deserves.

University of Sheffield R. J. WEBSTER

Statistics: A Guide to the Unknown. Edited by JUDITH M. TANUR, FREDERICK MOSTELLER ET AL. Wadsworth and Brooks/Cole, Pacific Grove, California, 1989. Pp. xxv+284. $16.95 (ISBN 0-534-09492-9).

This is an expanded and updated edition of a book first published in 1972, when a conference of teachers of children, teachers and undergraduates brought out a collection of essays explaining statistical ideas and methods without dwelling on their mathematical aspects: 'a bold stroke' to which they 'largely held firm'. The result has very little algebra but a few tables and graphs and is thereby (?) able to dwell on the background studies. I cannot improve on the blurb: 'deciding whether the sacrifice bunt and the intentional walk are good percentage baseball, determining the authorship of the Federalist papers, proving discrimination, determining royalties ... for music played on the radio, making unemployment estimates, determining how an astronomer ... can move a telescope efficiently from star to star, and how data of prehistoric quakes can be used to estimate the probability of large earthquakes.'

The result is highly readable and would interest sixth-formers as well as their teachers, besides giving solid background on sampling and its snags and on the drawing of conclusions from correlations. If all the protagonists in our present discussions on the National Health Service were to use statistics as thoughtfully and as ethically as those in this collection (which contains some very good essays on Health and Sickness and a Health Insurance experiment), we should feel confident about our future.

A final good touch is the threefold table of contents: (1) subject matter, (2) method of data collection and (3) statistical tools used. For those wanting more mathematics there is always excellent *Applied Statistics—Principles and Examples* by Cox and Snell, but get SAGTU first!

The Perse School, Cambridge J. L. G. PINHEY

The Games and Puzzles Journal. A bimonthly magazine edited and published by G. P. JELLIS, 99 Bohemia Road, St Leonards on Sea, East Sussex, TN37 6RJ. (ISSN 0267-369X). Annual subscription £6.

The *Games and Puzzles Journal* (GPJ) is a magazine with enormous variety. Each issue averages about 30 sides of condensed print. There are, for example, articles on new board games. I found a recent foray into the family of deceptively simple

Nim games particularly intriguing. The cover of another issue was printed with a board pattern to form the basis of a game invention competition. There are sections devoted to bridge and 'card play', and extensive coverage of the arcane world of chess. This provides a forum for setting competition problems and discussing composition and solutions. There are also articles on general chess topics such as new ideas for chess variants.

The remainder of the GPJ takes the form of discussion on the topic of various types of popular puzzle, reinforced in places by informal problem setting. There is quite a lot of feedback from readers. Stupendous dissections, magic squares, Latin squares, triangular billiards, cryptorithms, permutable primes ... The list is endless. Mathematical analysis of problems is somewhat limited, but nevertheless interesting. If other conundrums prove unyielding, a spell of light relief can be found in the final section entitled 'Word Play'. This always contains a cryptic crossword and a clutch of teasers, including a prize competition.

All in all the GPJ is great value; it is very stimulating and has its own unique charm.

Sixth Form, Oakham School DYLAN GOW

Penrose Tiles to Trapdoor Ciphers ... and the Return of Dr. Matrix. By MARTIN GARDNER. W. H. Freeman, Oxford, 1989. Pp. ix+311. 162 illustrations. Hardback £15.95 (ISBN 0-7167-1986-X), paperback £9.95 (ISBN 0-7167-1987-8).

Martin Gardner is rightly renowned for his mathematical column that appeared in *Scientific American* for nearly 25 years. These columns, expanded and updated, have provided the material for a sequence of books, of which this is the thirteenth. These books are unsurpassed as examples of how to write about mathematics for a mass readership. Nor does the quality diminish with time. In attempting to popularise mathematics there is a dilemma; should one reduce the mathematical detail and risk providing no more than a loose swirl of ideas, or retain the detail and thereby risk excluding all but a few from understanding what is written. Gardner treads an unerring path between these two extremes. There is enough in his writing to satisfy the mathematical appetite, but the text is never anything but clear for the non-specialist. Part of the trick is a careful choice of material. Gardner often writes about game theory, graph theory and other topics that require little background knowledge. The resulting text is distinctly modern, and in reading it one is made aware of the considerable amount of twentieth century mathematics that has sprung up largely independent of the classical tradition.

The Penrose tiles referred to in the title form a non-periodic tiling of the plane. Trapdoor ciphers are codes that are simple to encode but with a catch or 'trapdoor' that makes for very difficult decoding. Also covered are fractals and the games Nim and Eleusis. There is a splendid chapter on Ramsey theory and a fascinating account of Conway's surreal numbers that has sent me off to learn more. There are many other things to read about in this book, some informative and some lighthearted. The reading is easy and richly rewarding.

Penwith Sixth Form College, Penzance, Cornwall I. M. RICHARDS

CONTENTS

ISSN 0025-5653

PRICES (*postage included*)

Prices for Volume 23 (Issues Nos. 1, 2, 3 and 4)

Subscribers in	*Price per volume*	
North, Central and South America	US$13.00 or £8.00	(Note: These overseas prices apply even if the order is placed by an agent in Britain.)
Australia	$A16.00 or £8.00	
Britain, Europe and all other countries	£6.00	

A discount of 10% will be allowed on all orders for five or more copies of Volume 23 sent to the same address.

Details of reduced prices for two- and three-year subscriptions available on request.

Back issues

All back issues except Volume 1 are available; information concerning prices and a list of the articles published may be obtained from the Editor.

Enquiries about rates, subscriptions and advertisements should be directed to:

Editor—Mathematical Spectrum,
Hicks Building,
The University,
Sheffield S3 7RH, England.

Published by the Applied Probability Trust
Typeset by the University of Nottingham
Printed in England by Galliard (Printers) Ltd, Great Yarmouth