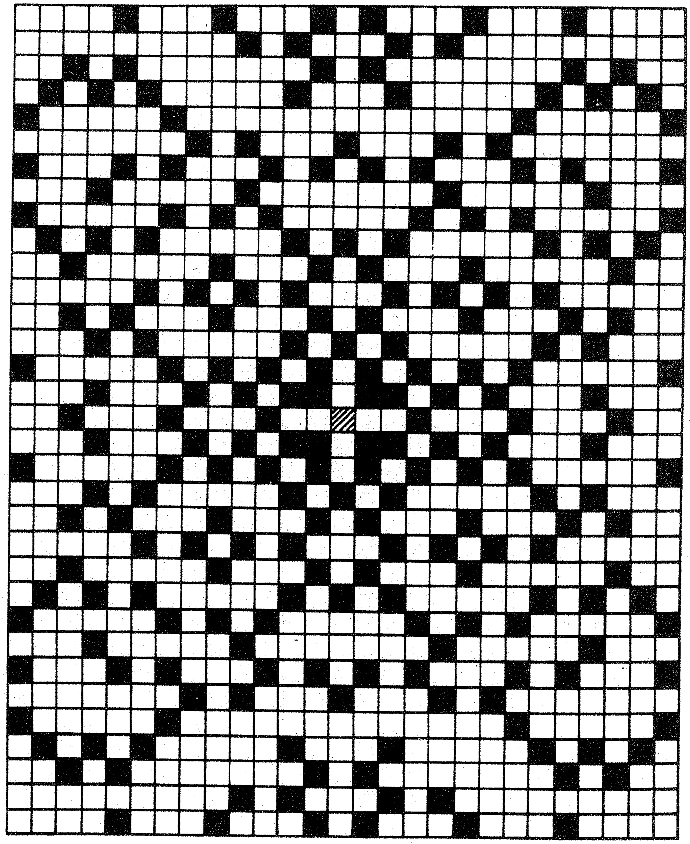
ISSN 0313-6825

FUNCTION

Volume 3 Part 5

October 1979



A SCHOOL MATHEMATICS MAGAZINE

Published by Monash University

Function is a mathematics magazine addressed principally to students in the upper forms of schools. Today mathematics is used in most of the sciences, physical, biological and social, in business management, in engineering. There are few human endeavours, from weather prediction to siting of traffic lights, that do not involve mathematics. *Function* contains articles describing some of these uses of mathematics. It also has articles, for entertainment and instruction, about mathematics and its history. Each issue contains problems and solutions are invited.

It is hoped that the student readers of *Function* will contribute material for publication. Articles, ideas, cartoons, comments, criticisms, advice are earnestly sought. Please send to the editors your views about what can be done to make *Function* more interesting for you.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

Articles, correspondence, problems (with or without solutions) and other material for publication are invited. Address them to:

The Editors,
Function,
Department of Mathematics,
Monash University,
Clayton, Victoria, 3168.

Alternatively correspondence may be addressed individually to any of the editors at the addresses shown above.

The magazine will be published five times a year in February, April, June, August, October. Price for five issues (including postage): $4.00; single issues $1.00. Payments should be sent to the business manager at the above address: cheques and money orders should be made payable to Monash University. Enquiries about advertising should be directed to the business manager.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

Registered for posting as a periodical - "Category B"

This issue carries two more schools' talks from the 1979 series and an excellent article taken from an address given about a year ago in Great Britain by Dame Kathleen Ollerenshaw, an eminent mathematician and educator. Dr Watterson's article describes a clever statistical technique due initially to S.L. Warner (1965), but subsequently improved by W.R. Simmons and others (1967). Our article describes the Simmons technique.

It is nice to see too that we have contributions from many readers on topics ranging from triangular chess to logarithmic approximation.

CONTENTS

The Front Cover. R.T. Worley 2

A Pathological Function. Neil Cameron 3

Primes. R.T. Worley 5

Laputa or Tlön. M.A.B. Deakin 11

Methods of Proof. Dame Kathleen Ollerenshaw 17

Too Embarrassed to Ask? G.A. Watterson 21

Letters to the Editor 22

Problem Section (Completed Solution to Problem 3.1.2;
Solutions to Problems 3.2.2, 3.2.3, 3.2.4, 3.2.7,
3.2.8, 3.3.1, 3.3.3, 3.3.4; Problems 3.5.1, 3.5.2,
3.5.3, 3.5.4) 26

Miscellanea 31

THE FRONT COVER

R. T. Worley, Monash University

When dealing with ordinary integers we classify certain numbers as primes. Namely, an integer p is called a prime if (i) p does not divide 1, (ii) p cannot be factored as a product $p = rs$ of integers except in the trivial ways where one of r,s is +1 or -1 (+1,-1 being the two integers that divide 1), and (iii) $p > 0$.

A number $m+ni$, where m,n are integers and $i^2 = -1$ is called a complex integer. $1 + 2i$ is a complex integer that can be factorized as a product of two complex integers only in the following ways:

$$\pm(1 + 2i)(\pm 1), \ (\pm 2 - i)(\pm i).$$

We note that one of the factors is ± 1 or $\pm i$, which are the four complex integers that divide 1. Furthermore, $1 + 2i$ does not divide 1, since $1/(1 + 2i) = \frac{1}{5} - \frac{2}{5}i$ is not an integer. We therefore call $1 + 2i$ a complex prime, or more correctly, a *Gaussian prime*, in view of the similarity of its properties with (i) and (ii) for ordinary primes. We shall call a complex integer a Gaussian prime if (i) it does not divide 1, and (ii) the integer only has trivial factorizations, where one of the factors is ± 1 or $\pm i$.

Factorization of complex integers is not difficult to perform, and we shall illustrate this by factoring $1 + 7i$. Let $1 + 7i = (a + ib)(c + id)$, so that $1 - 7i = (a - ib)(c - id)$. Then

$$50 = (1+7i)(1-7i) = (a+ib)(c+id)(a-ib)(c-id)=(a^2+b^2)(c^2+d^2).$$

Thus $a^2 + b^2$ must divide 50, and so must be 2,5,10 or 25 (not 1 or 50 as we are looking for non-trivial factorizations). Trying $a^2 + b^2 = 5$ gives $a + ib = \pm(2 \pm i), \pm(1 \pm 2i)$. Evaluating

$$(1+7i)/(2-i) = (1+7i)(2+i)/5 = (-5+15i)/5 = -1+3i,$$

so we have $(-1 + 3i)(2 - i) = 1 + 7i$.

The diagram on the cover is a representation of the Gaussian primes. Regarding the central hatched square as the origin (0,0), the square with coordinates (a,b) has been blackened to indicate that $a + ib$ is a Gaussian prime. The squares nearest the origin show that $\pm(1 \pm i)$, $\pm(1 \pm 2i)$, $\pm(2 \pm i)$, and ± 3, $\pm 3i$ are Gaussian primes, whereas $\pm(2 \pm 2i)$, $\pm(1 \pm 3i)$ and $\pm(3 \pm i)$ are not primes.

The symmetry of the diagram is due to the fact that whenever $a + ib$ is a prime, so also are $\pm(a \pm ib)$, $\pm i(a \pm ib)$. Another feature is that $p = p + 0i$ is a Gaussian prime for the ordinary integer p exactly when p is an ordinary prime of the form $4k + 3$ (e.g. 3,7,11,19,...). Integers of the form $a + ib$ with $a \neq 0$, $b \neq 0$ are Gaussian primes exactly when $a^2 + b^2 = 2$ or $a^2 + b^2$ is an ordinary prime of the form $4k + 1$.

Exercises: 1. Complete the factorization of $1 + 7i$ by factorizing $(-1 + 3i)$, which our diagram shows is not prime.

2. Factorize $6 + 8i$ as a product of primes.

3. Which primes divide both $1 + 7i$ and $6 + 8i$?

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

A PATHOLOGICAL FUNCTION

Neil Cameron, Monash University

It is not too hard to prove that between any two real numbers there is a *rational* number. First of all recall that, for an arbitrary real number x the *integer part* $[x]$ of x is that unique integer k such that $k \leqslant x < k + 1$, e.g. $[\pi] = 3$, $[\frac{55}{4}] = 13$ and $[-\sqrt{2}] = -2$.

Suppose x and y are real numbers and $x < y$ (so $y - x > 0$). Define the positive integer n and the integer m by

$$n = \left[\frac{1}{y - x}\right] + 1, \quad m = [nx] + 1.$$

Can you show, in general, that $x < p < y$ where p is the rational number $p = \frac{m}{n}$? As an example, with $x = \sqrt{2}$ and $y = \sqrt{3}$, we find $n = 4$, $m = 6$, $p = 1\frac{1}{2}$ and certainly $\sqrt{2} < 1\frac{1}{2} < \sqrt{3}$.

It follows that if $x < y$ then there are *two* rational numbers p and q, $x < p < q < y$. For example, with $x = \sqrt{2}$, $y = \sqrt{3}$, $p = 1\frac{1}{2}$ then applying the technique to $1\frac{1}{2}$ and $\sqrt{3}$ we find $q = 1\frac{3}{5}$.

We can now go on to show that between any two real numbers there is an *irrational* number. Again suppose x and y are real numbers and $x < y$. Then, as above, there are rational numbers p and q, $x < p < q < y$. Writing the positive rational number $q - p$ as $\frac{m}{n}$ where m,n are positive integers we see that $2n(q - p) = 2m$ is at least 2, so greater than $\sqrt{2}$. Therefore

$$q - p > \frac{\sqrt{2}}{2n} \text{ so } p < q + \frac{\sqrt{2}}{2n} < q.$$

Certainly $z = p + \frac{\sqrt{2}}{2n}$ is irrational: if it were rational then so would be $\frac{\sqrt{2}}{2n} = z - p$ and then $\sqrt{2} = \left(\frac{\sqrt{2}}{2n}\right) 2n$, but it was known to the Pythagoreans more than two thousand years ago that $\sqrt{2}$ is irrational. (This last result can be proved by supposing $\sqrt{2}$ is rational, writing $\sqrt{2}$ as $\frac{m}{n}$ where m and n are positive integers with no factor 2 in common and hence proceeding to a contradiction.)

Thus between any two real numbers there are both rational and irrational numbers. In particular if a is some fixed real number and δ is a positive real number then there are both rational and irrational numbers between a and $a + \delta$.

We can now give an example of a function whose domain is the set of all real numbers, which is very simple to define, whose graph is impossible to draw and which is not continuous anywhere, namely

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is a rational number,} \\ -1 & \text{if } x \text{ is an irrational number.} \end{cases}$$

Let a be a fixed real number and δ be an arbitrary positive real number. If a is rational then as above there is an irrational number, say x, between a and $a + \delta$ so $f(a) - f(x) = 1 - (-1) = 2$; if a is irrational then similarly there is a rational number, say x, between a and $a + \delta$ so $f(x) - f(a) = 1 - (-1) = 2$. Thus in either case there exist numbers x arbitrarily close to a where the absolute difference $|f(x) - f(a)|$ is 2. At an intuitive level, we see then that $f(x)$ cannot tend to $f(a)$ as x tends to a. Formally, for a real-valued function g, continuity at a real number a means:

> *for* each *positive (εrror tolerance)* ε*, there is a suitably small positive (δifference)* $\delta = \delta(\varepsilon)$ *such that* $g(x)$ *differs from* $g(a)$ *by less than* ε *whenever* x *differs from* a *by less than* δ.

Thus f does not satisfy this condition for $\varepsilon \leqslant 2$, so is not continuous at a. But a was simply any real number, so f is not continuous anywhere!

Problem: Show that between any two real numbers there are *infinitely* many rational numbers and *infinitely* many irrational numbers.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

PROBLEMS OF DEFINITION

There are certain notions which it is impossible to define adequately. Such notions are found to be those based on universal experience. Probability is such a notion. The dictionary tells me that 'probable' means 'likely'. Further reference gives the not very helpful information that 'likely' means 'probable'.

- *Facts from Figures*, M.J. Moroney, 1951.

PRIMES

R.T. Worley, Monash University

Prime numbers are perhaps the most studied of all natural numbers. Besides being the basic building blocks from which all integers greater than 1 may be formed by multiplication, primes have other interesting properties which make them useful in surprising ways. The study of primes is not always easy, because while they occur with reasonable regularity, their occurrence is still sufficiently irregular to make things difficult. Indeed, one authority, Don Zagier, likened the occurrence of primes in the list of integers to the appearance of weeds in a field. Although you know there are more to appear, you cannot tell where the next one will sprout. A glance at the following table, where the primes have been lowered, will show what he meant.

1 $_{2}$ $_{3}$ 4 $_{5}$ 6 $_{7}$ 8 9 10 $_{11}$ 12 $_{13}$ 14 15 16 $_{17}$ 18 $_{19}$ 20 21 22 $_{23}$ 24

25 26 27 28 $_{29}$ 30 $_{31}$ 32 33 34 35 36 $_{37}$ 38 39 40 $_{41}$ 42 $_{43}$ 44 45

46 $_{47}$ 48 49 50 51 52 $_{53}$ 54 55 56 57 58 $_{59}$ 60.

The following table indicates that this irregularity does not confine itself to small numbers.

Primes between $10^7 - 100$ and 10^7: 9 999 901, 9 999 907, 9 999 929, 9 999 931, 9 999 937, 9 999 943, 9 999 971, 9 999 973, 9 999 991.

Primes between 10^7 and $10^7 + 100$: 10 000 019, 10 100 079.

However, despite this irregularity, there is still some regularity as is shown by the following table. In this table, $\pi(x)$ denotes the number of primes less than or equal to x. For example, $\pi(10) = 4$ because there are four primes $p \leqslant 10$, namely $p = 2$, $p = 3$, $p = 5$, $p = 7$.

x	$\pi(x)$	$\pi(x)\log_e x$	$\dfrac{\pi(x)\log_e(x)}{x}$
10	4	9·21	0·921
100	25	115·13...	1·15...
1000	168	1160·5...	1·16...
10^4	1 229	$1.131\ldots\times10^4$	1·131...
10^5	9 592	$1.104\ldots\times10^5$	1·104...
10^6	78 498	$1.084\ldots\times10^6$	1·084...
10^7	664 579	$1.071\ldots\times10^7$	1·071...
10^8	5 761 455	$1.061\ldots\times10^8$	1·061...
10^9	50 847 534	$1.053\ldots\times10^9$	1·053...
10^{10}	455 052 512	$1.047\ldots\times10^{10}$	1·047...

[†] Text of a schools' lecture delivered on July 20, 1979. For other articles on primes, see *Function*, Vol.2, Part 4 and Vol.3, Parts 1,4.

From this table it seems that $\pi(x)$ and $x/\log_e x$ are related. The fact that $\pi(x).\log_e(x)/x \to 1$ as $x \to \infty$ was discovered by Gauss in 1792, but was not proved till over a century later.

The fact that there are infinitely many primes has a fairly simple proof, and we can show that there are arbitrarily long gaps between consecutive primes by a small addition to the proof. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\ldots, p_n$ be the first n primes, and let N_n denote their product. That is,

$$N_n = 2.3.5.7. \ldots .p_n .$$

Then none of $2, 3, \ldots, p_n$ divide $N_n + 1$, for if p divides N_n and $N_n + 1$ then p would have to divide the difference, i.e. divides 1. Hence there must be at least one more prime (one dividing $N_n + 1$). In this way we keep producing more and more primes, showing that there are infinitely many. Now consider the consecutive numbers $N_n + 2$, $N_n + 3$, $N_n + 4$, $\ldots$, $N_n + p_n$. It is easy to see that none of these are prime. Consider for example $N_n + m$. Since $m \leqslant p_n$, it has a prime divisor $p \leqslant p_n$. But then p must be one of $p_1, \ldots, p_n$ and so p also divides N_n. Thus p divides $N_n + m$. We have therefore constructed a string of $p_n - 1$ consecutive numbers that are not prime.

For many years people have looked for a formula for primes, but no useful formula has been found. Centuries ago it was thought that $p(n) = n^2 + n + 41$ gave only primes for integral $n \geqslant 1$. Certainly it does for $n = 0, 1, 2, \ldots, 39$, but it doesn't for $m = 40$, $m = 41$ when 41 divides $p(m)$. Indeed, no polynomial can give only prime numbers as values. However, recently mathematical logicians have shown that the polynomial below, in 26 integer variables, has as its positive values precisely all the primes.

$$\begin{aligned}
F(a,b,c,d,\ldots,w,x,y,z) = [k+1]\,[1 &- (wz+h+j-q)^2-(2n+p+q+z-e)^2 \\
&- (a^2y^2-y^2+1-x^2)^2 \\
&- (\{e^4+2e^3\}\{a+1\}^2+1-o^2)^2 \\
&- (16\{k+1\}^3\{k+2\}\{n+1\}^2+1-f^2)^2 \\
&- (\{\langle a+u^4-au^2\rangle^2-1\}\{n+4dy\}^2+1- \\
&\quad -\{x+cu\}^2)^2 - (ai+k+1-\ell-i)^2 \\
&- (\{gk+2g+k+1\}\{h+j\}+h-z)^2 \\
&- (16r^2y^4\{a^2-1\}+1-u^2)^2 \\
&- (p-m+\ell\{a+n-1\}+b\{2an+2a-n^2-2n-2\})^2 \\
&- (z-pm+p\ell a-p^2\ell+t\{2ap-p^2-1\})^2 \\
&- (q-x+y\{a-p-1\}+s\{2ap+2a-p^2-2p-2\})^2 \\
&- (a^2\ell^2-\ell^2+1-m^2)^2 - (n+\ell+v-y)^2]
\end{aligned}$$

Other formulae for giving primes have been suggested. Fermat (1601-1665) conjectured that

$$F_n = 2^{2^n} + 1$$

is prime for integral $n \geqslant 0$. Certainly $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$

and F_4=65 537 are prime, but F_5=4 294 967 297 is not, being divisible by 641. In fact no other F_n are known to be prime, but some others are known to be composite.

[Exercise. Multiply out

$$(2^9 + 2^7 + 1)(2^{23} - 2^{21} + 2^{19} - 2^{17} + 2^{14} - 2^9 - 2^7 + 1)$$

to get $2^{32} + 1$.]

Mersenne, in 1644, conjectured that

$$M_p = 2^p - 1$$

is prime for prime p. However this is false since, while $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ and $M_7 = 127$ are prime, $M_{11} = 2047$ is divisible by 23. These numbers have been investigated deeply as there are ways of testing for their primality. One of these is due to Lucas, who showed that M_p is prime if and only if M_p divides L_{p-1}, where $L_1 = 4$, $L_2 = 4^2 - 2 = 14$, $L_3 = 14^2 - 2 = 194$, $L_4 = 194^2 - 2 = 37\ 634$, ..., $L_n = L_{n-1}^2 - 2, \ldots$. In 1876 Lucas showed 2^{127}-1=170 141 183 460 469 231 731 687 303 715 884 105 727 was prime. This was the largest known prime, and held that record for many years. In fact it was only the advent of electronic computers that led to larger primes being discovered. The following table lists the larger primes that have been discovered.

p	No.of digits	Year	p	No.of digits	Year
$2^{127}-1$	39	1876	$2^{4253}-1$	1281	1961
$114(2^{127}-1)+1$	41	1951	$2^{4423}-1$	1332	1961
$\frac{1}{17}(2^{148}+1)$	44	1951	$2^{9689}-1$	2917	1963
$180(2^{127}-1)^2+1$	79	1951	$2^{9941}-1$	2993	1963
$2^{521}-1$	157	1952	$2^{11213}-1$	3376	1963
$2^{607}-1$	183	1952	$2^{19937}-1$	6002	1971
$2^{1279}-1$	386	1952	$2^{21701}-1$	6533	1978
$2^{2203}-1$	664	1952	$2^{23209}-1$	6987	1978
$2^{2281}-1$	687	1952	$2^{44497}-1$	13395	1979
$2^{3217}-1$	969	1957			

There are now 27 known Mersenne primes. Such primes are of interest because of their relation to perfect numbers. A perfect number is a positive integer $n \geqslant 2$ for which the sum of the positive divisors of n is $2n$. For example 6 has divisors 1,2,3,6 whose sum is 12, while 28 has divisors 1,2,4,7,14,28 whose sum is 56. It is known that an even number is perfect exactly when it has the form $2^{p-1}M_p$ where M_p is prime. Thus, besides 6 and 28, other perfect numbers are 16 × 31, 64 × 127, ..., $2^{44496}(2^{44497}-1)$. Since no odd perfect numbers are known, there are precisely 27 known perfect numbers.

It is easy to show that M_n is not prime if n is not prime. If $n = st$, where $s \geqslant 2$, $t \geqslant 2$, then in the formula

$$(a^r - 1) = (a - 1)(a^{r-1}+a^{r-2}+\dots+a^2+a+1)$$

we set $a = 2^s$, $r = t$ to obtain

$$(2^s)^t - 1 = (2^s - 1)(1+2^s+2^{2s}+\dots+2^{(t-1)s}),$$

which gives a factorisation of $2^n - 1$.

[Exercise. Show that $2^m + 1$ is not prime if m is not a power of 2 (i.e. if m is divisible by an odd prime q).]

We shall now look at some of the properties of primes. It is easy to see that the prime p divides the binomial coefficient $\binom{p}{r}$ for $r = 1,2,\dots,p-1$, for

$$\binom{p}{r} = \frac{p(p-1)\dots(p-r+1)}{r(r-1)\dots 2.1}$$

as each of $1,2,\dots,r$ is less than p. Using this fact, we can show that p divides $n^p - n$ for every integer $n \geqslant 1$. A couple of cases will illustrate this.

Firstly, $1^p - 1 = 0$ is divisible by p. Secondly, by the Binomial theorem,

$$2^p-2 = (1+1)^p-2 = 1^p+\binom{p}{1}1^{p-1}.1+\binom{p}{2}1^{p-2}.1^2+\dots+\binom{p}{p-1}1.1^p+1^p-2$$

$$= \binom{p}{1} + \binom{p}{2} + \dots + \binom{p}{p-1}.$$

Since each binomial coefficient is divisible by p, so is the sum $\binom{p}{1} + \dots + \binom{p}{p-1}$. Thirdly

$$3^p-3 = (2+1)^p-3 = 2^p+\binom{p}{1}2^{p-1}.1+\dots+\binom{p}{p-1}2.1^{p-1}+1^p-3$$

$$= (2^p-2)+2^{p-1}\binom{p}{1}+\dots+2\binom{p}{p-1},$$

and once again each term on the right is divisible by p. This process can be continued indefinitely.

Since p divides $n(n^{p-1} - 1)$, it is clear that, if p does not divide n, then p divides $n^{p-1} - 1$. In particular, p divides $2^{p-1} - 1$ for $p \neq 2$. 25 centuries ago the Chinese believed that an odd number q was prime if and only if q divides $2^{q-1} - 1$. This belief lasted for more than 23 centuries. The smallest q for which this fails is $q = 341$. We call a number q a pseudoprime if it is not a prime but q divides $2^q - 2$. 561 is another pseudoprime which has the property that 561 divides $n^{561} - n$ for every integer n. The first even pseudoprime, 161038, was discovered in 1950.

Recently large prime numbers have been used in coding of secret messages. To understand how this works we shall look at remainders. If p is a prime, then for an integer m we divide m

by p, and let m_p denote the remainder. A few examples will explain this:

$$\begin{aligned} 5 &= 0 \times 7 + 5 & \therefore\quad 5_7 &= 5 \\ 33 &= 4 \times 7 + 5 & \therefore\quad 33_7 &= 5 \\ 172 &= 24 \times 7 + 4 & \therefore\quad 172_7 &= 4 \\ 21 &= 3 \times 7 + 0 & \therefore\quad 21_7 &= 0. \end{aligned}$$

Remainders of large numbers can be calculated quite easily, making use of the formula $(ab)_p = (a_p . b_p)_p$. Once again some examples will illustrate this.

$$(33\times172)_7 = (33_7\times172_7)_7 = (5\times4)_7 = 20_7 = 6$$

$$(33^2)_7 = (33\times33)_7 = (33_7\times33_7)_7 = (5\times5)_7 = 25_7 = 4$$

$$(33^4)_7 = (33^2\times33^2)_7 = ((33^2)_7\times(33^2)_7)_7 = (4\times4)_7 = 16_7 = 2.$$

We have already seen that, if p does not divide n, then p divides $n^{p-1} - 1$. In other words $(n^{p-1})_p = 1$. Now suppose that c and d are numbers such that, for some integer k,

$$cd = k(p - 1) + 1,$$

i.e. cd is one more than a multiple of $p - 1$. Then

$$\begin{aligned} \left((n^c)^d\right)_p = (n^{cd})_p &= (n^{k(p-1)+1})_p \\ &= \left(n^{k(p-1)}_p . n_p\right)_p \\ &= \left(\left(n_p^{p-1}\right)^k . n_p\right)_p \\ &= (1.n_p)_p \\ &= n_p . \end{aligned}$$

To see how this can be used in developing a code, we let p be a large prime, and let the message be converted into a number n less than p,

$$\text{e.g.}\quad \begin{matrix} H & E & L & P \\ 08 & 05 & 12 & 16 \end{matrix}\ , \qquad p = 10\ 000\ 019.$$

We then choose a coding number c and decoder d, for example

$$c = 3,\ d = 66\ 666\ 679, \text{ so that } cd = 2(10\ 000\ 018) + 1.$$

The agent calculates

$$(n^3)_p = (8\ 05\ 12\ 16^3)_p \doteq m$$

and sends that number. The headquarters than calculates

$$(m^{66\ 666\ 679})_p = n_p .$$

But $n_p = n$ (because $n < p$), so headquarters has the message. Of course the calculation of $m^{66\ 666\ 679}$ is simple, using the formula mentioned above, in these days of computers. The above code is not the one actually used, for if the enemy captures one agent he has c and p. It is then easy to work out d and so he can decode all messages from other agents. In practice a number P, the product of two distinct primes q_1q_2 is used in place of p. After choosing a coding exponent C a decoding exponent D can be worked out (so that $CD = k(q_1-1)(q_2-1)+1$) and the above procedure followed. Because D cannot be worked out easily even when C and P have been discovered this procedure is very safe. In practice q_1 and q_2 have around 100 digits each, and since it will take even the fastest computer to date over a year to find the factors of P the code cannot be broken easily. Another advantage of this code is that it is reversible. If headquarters wants to send out a message m, it computes $(m^D)_p$ and sends that out. The agent calculates $((m^D)_p^C)_p$ and has m. Since only headquarters knows D, the agent is sure the message is genuine.

Some of the details are taken from an article in *The Mathematical Intelligencer*, Vol.0, 1977. For more on coding see *Function*, Vol.2, Part 4, and *Scientific American*, August 1977.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

PERCENTAGES

... since 1970 the number of students taking a "science" HSC - ... - has declined more than 16%.

Whereas in 1970 one in every six HSC students took a science HSC, today fewer than one in 10 does so.

Geoff Maslen, Education Editor, *The Age*,
Friday, 29 June, 1979, p.5.

If the decrease in numbers taking science HSC from 1970 to now is exactly 16%, show that the statement of the last paragraph shows that there has been a 40% increase in the number of HSC candidates since 1970.

[In fact the increase has not been this great; the discrepancy would appear to be due to roundoff errors in the data.]

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

FROM A REVIEW

There is much that he does not say that he means, that he knows you know he means, and so you cannot contradict what he does not say, what you know he means to say - and yet you cannot agree with what he does say, for you know that that will be taken to mean that you agree with what he does not say as well, and to that you are firmly opposed. I hope the reader will survive this. That is how I felt after reading [this book].

Mathematical Gazette, 1916.

LAPUTA OR TLÖN ?[†]

M.A.B. Deakin, Monash University

My title gives two possible answers to the question: "What kind of dream-world do you mathematicians inhabit?" We sometimes find ourselves relegated to "Cloud Nine", "off the planet", etc. Some of the public - even the influential public - see pure mathematics as consisting of airy-fairy flights of imagination indulged in by a few rare nuts of a freakish turn of mind. Such a view places us in *Laputa*. Some of you may know of it. After Gulliver had left the mini-micro world of Lilliput, and had done with the super-dooper extra Texans of Brobdignag, he visited several places, among them a land of airborne floating islands, peopled by impossibly impractical researchers. This was *Laputa*.

This land does not exist, being a product of Jonathon Swift's embittered and satirical mind. Nonetheless, it is very real, for it stands as a symbol of impractical and dilettantish research. *Laputa* lives on as an image of the most convolutedly abstract, narrowly academic, deliberately useless thinking that mankind can produce.

Mathematicians do not, outside the realms of fiction, inhabit *Laputa*.

We live, in fact, in *Tlön* - a world at once much more dreamy and abstract, much more here and now, and much less known to the average reader of this article. *Tlön* is a fictitious land, the invention of the *heresiarchs of Uqbar*, a country which also does not exist. *Uqbar* was the result of a conspiracy by a secret society known as *Orbis Tertius* - itself a fiction invented by the Nobel Laureate, Jorge Luis Borges, who, you will by now be pleased to hear, is alive and well, and living in Argentina.

Tlön is thus a $(\text{fiction})^3$, and yet it is our reality, for it is Borges' symbol of the way in which intellectual frameworks affect our perception of the world. (I shall not, in an essentially mathematical article, enter the controversy over the metaphysics or the theology of *Tlön*.) Mathematics in its development affects and is affected by the intellectual framework we inherit.

Had Swift been told in 1726 that mathematicians were investigating the square root of -1, he would undoubtedly have relegated them to *Laputa*. In point of mathematical nicety, as subtraction is a simpler operation than division, negative numbers, arising from the former, logically precede fractions, owing their genesis to the latter.

[†] Text of a schools' lecture delivered on August 3, 1979.

None of which, of course, reflects the actual sequence of historical acceptance. The Greeks of Pythagoras' time had not only fractions, but irrational numbers. Yet 23 centuries later, Euler regarded negative numbers as "imaginary quantities". The point is that I can imagine (for example) $\frac{3}{4}$ of an apple, without undue mental strain. To imagine -1 apple, however, involves my envisioning some sort of "hole" in the fabric of the universe.

In discussing the square roots of such quantities, we enter a world of unreality that daunted our mathematical forebears. To this day, we speak of "real numbers" and "imaginary numbers" - the latter being those that, when squared, give rise to a negative (nowadays respectably real) number. A "complex number" is the sum of a real and an imaginary number.

Now, you may have been told, or you may have imagined for yourself, that complex numbers were invented because of some aesthetic need for completeness. The equation

$$x^2 - 1 = 0$$

has two solutions, while

$$x^2 + 1 = 0$$

has none. We are being unfair to the second equation.

Life was never so simple. The point is rather different, insofar as historians have been able to piece it together (and this is a difficult matter).

Consider the quadratic equation

$$ax^2 + bx + c = 0.$$

You and I know that we can solve this by, if all else fails, using the formula

$$x = \frac{1}{2a}\{-b \pm \sqrt{b^2 - 4ac}\} ,$$

if $b^2 > 4ac$.

This much was known to the Greeks of antiquity. It was the genius of Renaissance Italy to solve the next problem in line - to wit

$$ax^3 + bx^2 + cx + d = 0.$$

It is possible simply to write down a formula (a very messy one) for the roots of this equation. But no understanding lies that way. Let us first simplify the problem. Observe, to begin with, that we can divide through by a (unless, of course, $a = 0$, a trivial case).

This gives, with change of notation,

$$x^3 + Ax^2 + Bx + C = 0.$$

This form of the equation may be simplified yet further.

I will deal with two specific examples:

$$x^3 - 3x^2 + 6x - 8 = 0 \qquad (1)$$

$$x^3 + 6x^2 - 9x -14 = 0. \qquad (2)$$

To simplify Equation (1), put $x = y + h$. This yields

$$y^3 + (3h-3)y^2 + (3h^2-6h+6)y + (h^3-3h^2+6h-8) = 0.$$

Now choose $h = 1$, to produce

$$y^3 + 3y - 4 = 0. \qquad (3)$$

A similar process applied to Equation (2) gives (with $h = -2$)

$$y^3 - 21y + 20 = 0. \qquad (4)$$

You may check that Equation (3) has the single root $y = 1$ (i.e. $x = 2$), and Equation (4) has three roots $y = -5,1,4$ (i.e. $x = -7,-1,2$).

We may similarly reduce all cubic equations to the standard form

$$y^3 + 3Hy + G = 0. \qquad (5)$$

The solution of Equation (5) is nowadays widely attributed to the Italian mathematician Tartaglia (1500? - 1577), although there is some dispute about this among historians of mathematics.

The key insight now is the observation that

$$y^3-3pqy+(p^3+q^3) = (y+p+q)(y^2-[p+q]y+[p^2+q^2-pq]). \qquad (6)$$

(You may easily check this factorisation.) It follows that the equation

$$y^3 - 3pqy + (p^3 + q^3) = 0 \qquad (7)$$

may be solved. One root is $y = -(p + q)$. The others (if present) may be found by setting the quadratic factor equal to zero.

Now compare Equations (5) and (7). Equation (5) may be solved if we can determine p,q to satisfy

$$pq = -H,\ p^3 + q^3 = G,$$

or

$$p^3q^3 = -H^3, p^3 + q^3 = G.$$

p^3, q^3 are thus the roots of a quadratic equation

$$t^2 - Gt - H^3 = 0.$$

(This holds because $(t - p^3)(t - q^3) = t^2 - (p^3 + q^3)t + p^3q^3$.)

It follows that

$$p = \{\tfrac{1}{2}[G + \sqrt{G^2 + 4H^3}]\}^{1/3}$$

$$q = \{\tfrac{1}{2}[G - \sqrt{G^2 + 4H^3}]\}^{1/3}$$

Applying this procedure to Equation (3), for which $H = 1$, $G = -4$, we find, after some work, $p = (\sqrt{5} - 2)^{1/3}$, $q = -(\sqrt{5} + 2)^{1/3}$. We may now check that $p = \tfrac{1}{2}(\sqrt{5} - 1)$, $q = -\tfrac{1}{2}(\sqrt{5} + 1)$. As the root y is $-(p + q)$, we find

$$y = -\tfrac{1}{2}(\sqrt{5} - 1) + \tfrac{1}{2}(\sqrt{5} + 1) = 1,$$

as expected.

Turn now to Equation (4). In this instance $H = -7$, $G = 20$, so that we reach

$$p = \{10 + q\sqrt{-3}\}^{1/3}$$

$$q = \{10 - q\sqrt{-3}\}^{1/3}$$

We can proceed no further, as our formulae involve the dreaded square roots of negative numbers. (This is all the more maddening, as we know that three perfectly respectable real roots are there waiting for us in the wings.)

The decisive step seems to have been taken by another Italian mathematician, Bombelli (1526-1572). Writing i for $\sqrt{-1}$, without thought to whether or not i exists, we may discover

$$p = -\tfrac{1}{2} + \frac{3\sqrt{3}}{2}\,i$$

$$q = -\tfrac{1}{2} - \frac{3\sqrt{3}}{2}\,i\ ,$$

results which may be checked by cubing and writing -1 in place of i^2, wherever it occurs.

Now we put $y = -(p + q) = \tfrac{1}{2} - \frac{3\sqrt{3}}{2}\,i + \tfrac{1}{2} + \frac{3\sqrt{3}}{2}\,i = 1$, which is one of the three roots. Note, however, that to find this *real* root, we *had* to have recourse to complex numbers. (It is a theorem, and you can prove it from the formulae given in this article, that this is always the case when a cubic has three real roots.) Bombelli passed through the valley of the shadow and emerged unscathed. To re-enter reality, he had to travel through Tlön.

But once Tlön has been sighted, be it ever so briefly, there is no turning back. Like all early voyagers, he left confused maps and log books. "I have found", he wrote, "a new sort of cube root, easily distinguished from the others". What he had found (haven't we just been saying it?) was a new sort of square root.

The matter depends on how you see it. We look back on Bombelli's achievement with four centuries of cheaply inherited wisdom. Naturally he had discovered cube roots. After all, they cropped up in connection with cubic equations. Any old fool can write $i^2 = -1$, and even invent a play algebra around it. He will inhabit Laputa and never sight Tlön. To qualify for residence in Tlön, one needs not only to entertain zany ideas, but to know what to do with them, and how to tame them to human purposes.

Let us take a simple cubic - a very simple one, namely $x^3 - 1 = 0$. This is readily factorised to give

$$(x - 1)(x^2 + x + 1) = 0$$

and we recover the solitary root $x = 1$, as we should expect. But now we have the possibility that

$$x^2 + x + 1 = 0. \qquad (8)$$

We cannot shirk it, as our earlier excuse, that square roots of negative numbers do not exist, no longer holds water. We have ourselves gainsaid it.

We apply the formula to Equation (8), to find

$$x = -\tfrac{1}{2} \pm \frac{\sqrt{3}}{2} i.$$

We may write $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i$ and check that $\omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2} i$. $\omega^3 = 1$, as we may verify the matter by calculation; $(\omega^2)^3 = 1$ also.

A similar analysis may be applied to the quadratic factor in Equation (6). This now factorises into

$$(y + \omega p + \omega^2 q)(y + \omega^2 p + \omega q).$$

Equation (7) has two other roots besides $y = -(p + q)$. They are $y = -(\omega p + \omega^2 q)$ and $y = -(\omega^2 p + \omega q)$. I leave it as an exercise to you, the reader, to check that in Equation (4), these produce for us $y = -5$ and $y = 4$, the two other roots whose whereabouts may have troubled you.

Our picture is still unsatisfactory, however. It is still possible to object that all this is very fine, but that these calculations involving i are disreputable and suspect, because i does not exist. The objection is, in essence, that, thinking to find Tlön, we have drifted off to Laputa. What is required is a proof that the imaginary numbers are every bit as real as the real numbers.

We need to show that it is possible to represent complex numbers and their properties entirely in terms of the properties of the more familiar real numbers. The first successful proof along these lines was due to Carl Friedrich Gauss (1777-1855), who is often regarded with Archimedes and Newton as one of the very greatest mathematicians of all time.

Modern texts, however, tend to follow a later and simpler treatment, due to Hamilton (1805-1865). On this account, complex numbers are pairs of real numbers $[a,b]$ that add and multiply according to the laws

$$[a,b] + [c,d] = [a + c,\ b + d]$$

$$[a,b] \ . \ [c,d] = [ac - bd,\ ad + bc] \ .$$

The imaginary numbers are those pairs $[0,b]$, for which the first number is zero, and i is an abbreviation for $[0,1]$. We may now calculate i^2 as $[0,1] \ . \ [0,1]$, whose value is found quite readily to be $[-1,0]$.

This is not exactly the real number -1, but is so close to it in behaviour that we abbreviate it to -1. A similar convention applies in the case of any other complex number whose second member is zero. These numbers are referred to as "real", although there is a slight misuse of language involved here.

The point of these manoevres is that they demonstrate conclusively that there is no mystery to the complex numbers, after all. We can happily use them, as Bombelli did and know we're not talking nonsense. We will be safe living in Tlön.

That we have come to live there is perhaps best indicated by the fact that those eminent realists, the electrical engineers, treat alternating currents and voltages as complex quantities, and combine the resistance, inductance and capacitance of a circuit into one complex quantity - the impedance. $\sqrt{-1}$ is here to stay.

Further Reading

Gulliver's voyage to Laputa is described in Book Three of *Gulliver's Travels*, which should be readily accessible to the reader. Tlön is described in the short story *Tlön, Uqbar, Orbis Tertius*, which is less widely available. The best English translation is to be found in the collection *Labyrinths*, edited by D.A. Yates and J.E. Kirby and published in the Penguin Modern Classics series.

My account of complex numbers and the solution of cubic equations is based on that given by C.V. Durell and A. Robson in *Modern Algebra, Vol.* II, published in 1937. Modern treatments of complex numbers are easily accessible. There are not so many good treatments of cubic equations. However, *College Algebra*, by J.R. Rosenbach, E.A. Whitman, B.E. Meserve and P.M. Whitman (published by Ginn) has a good account.

My treatment of the history of these matters is based on a study by my colleague, J.N. Crossley, and available from him. A recent study is P.L. Rose's *The Italian Renaissance of Mathematics*.

The electrical uses of $\sqrt{-1}$ are to be found in almost any standard text on A.C. Circuit Theory. In this context, i represents current and $\sqrt{-1}$ is denoted by j. ω is angular frequency, and hence is not used to abbreviate $(-1 + \sqrt{-3})/2$.

METHODS OF PROOF

Dame Kathleen Ollerenshaw,
Institute of Mathematics
and its Applications†

There are several recognised methods of mathematical proof, but proof is never absolute and there are varying degrees of rigour. A mathematical proof is only valid within the limits of the definitions laid down. We can change the rules or move the goal posts in mathematics as surely as we do in other evolving activities and start an entirely new ball game, often very fruitfully. Geometrical truths, though eternal in a Euclidean world, did not suffice for the geometry of outer space. Proof may traditionally be by the "direct method" (as with Pythagoras's theorem); by one of the indirect methods such as *reductio ad absurdum*; or by inversion or translation from other known results; or by the method of exhaustion of all possibilities. An example of the latter is the standard proof that there can be (and are) only five regular Platonic Solids - the tetrahedron, the cube, the octahedron, the dodecahedron and the icosahedron. Sir Hermann Bondi and I used this method when solving and finding the correct answer to the classical *Nine Prisoners Problem* this time last year.†† The recently accomplished computer-crushing solution to the famous *Four Colour Map Problem* is an example of proof by exhaustion of defined possibilities.#

As an example of proof by translation, in this instance by projective geometry, here is one of the most beautiful results of all mathematics found by Pascal (1623 - 1662) at the age of 16.

Pascal's theorem states that:

If a hexagon is such that its six points of intersection lie on any conic, then the three points of intersection of opposite sides lie on one straight line.

† A professional organisation of mathematicians, based in the U.K. This article is excerpted from Dame Kathleen's presidential address, entitled *The Magic of Mathematics*, and is reproduced, with permission, from the Institute's *Bulletin* (Vol.15, No.1, Jan.1979).

†† i.e. 1977.

See *Function*, Vol.1, No.1.

The points can be taken in any order (Fig.1). The theorem can be proved by using "cross-ratios" (which I shall not explain here) and for the simplest of the conics - the circle. By projection this establishes its truth for all conics as cross-ratios remain invariant under projection and all conics are projections of one another.

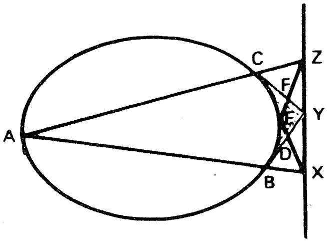


Figure 1.

The result is astonishing, beautiful and of great generality, and the proof is elegance itself. To add to the magic, 144 years after the death of Pascal in 1662, another Frenchman, C.W. Brianchon, when still a student, discovered by means of the "principle of duality" a related theorem.

Brianchon's theorem states that:

If a hexagon formed by six straight lines is such that they are tangents to a conic, then the three lines joining opposite vertices intersect at a point (Fig.2).

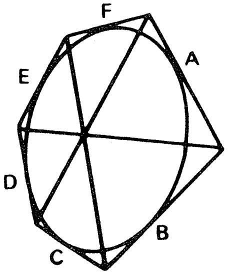


Figure 2.

The figures for these two propositions do not look alike, which emphasises the power of the particular method of proof employed, in which one result is deduced from the other.

I had thought to show you several classical proofs of special beauty. I shall ration myself to just two, the first in probability which I came across for the first time only recently. This is known as *Buffon's Needle Problem*. In a Sultan's palace the floors were tiled to give thin parallel lines, narrowly spaced at a distance d apart. The ladies of the harem would keep dropping their embroidery needles. The Sultan decided to lay bets on the probability of a needle when dropped crossing a line. If the length of the needle is l, $l < d$, what odds was he to lay to be sure over time of being the winner? Buffon's solution involves the multiplication of two probabilities and a difficult integration, the answer being $2l/\pi d$. Buffon died in 1788. More than a hundred years later another Frenchman, Rabier, provided a marvellously simple method of arriving at the same solution. I use Rabier's description as quoted in Coolidges's "Mathematics of the Great Amateurs." "The probability of the needle crossing a line is the expectation of a man who is to receive one crown if a crossing takes place. This expectation is the sum of the expectations of the various elements of the needle, and these are unaltered if the needle is bent into a circle. The probability of a crossing is now the ratio of the diameter of this circle, namely l/π, to d, the distance between the lines. But if the bent needle crosses a line once, it will cross it twice, so the expectation is $2l/\pi d$" (Fig.3). I had a real thrill out of this and I have revelled in it - a difficult problem until Rabier thought of bending the needle into a circle, rather like Christopher Columbus and the egg.

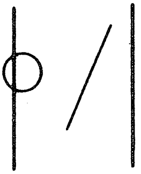


Figure 3.

The second example is simpler. In the February 1978 *Bulletin*[†] Professor Patterson of Aberdeen at the end of an article about "Mathematical Challenge," the competition initiated in Scotland for sixth-formers, put forward a problem. I quote: "Consider the game of noughts and crosses. In how many ways can a line of three noughts or three crosses be achieved? The answer is eight. There is a three-dimensional version (trade-named Plato). This has 27 holes and two players each with a set of coloured marbles who place these in turn in the holes. The winner is the player who achieves, when all the holes are filled, the larger number of rows-of-three in any direction. Question: How many different ways are there of achieving a row of three?" The makers of the game give an incorrect answer 48, whereas by counting carefully and remembering the diagonals we can check that there are 49. The problem Professor Patterson posed was to extend this to n dimensions and to give the number of rows-of-three in an n-dimensional hypercube. Several people sent the correct answer, most by inelegant methods or in inelegant form, but a proof sent by Dr David Singmaster, which it later transpired had already been given in 1941 in the *Scientific American*, has a delightful simplicity.

[†] The *Bulletin of the Institute of Mathematics and its Applications*.

Consider first the two-dimensional noughts-and-crosses matrix (Fig.4). There are nine positions represented here by the nine little circles or "holes". The three horizontal rows of holes, three vertical rows and two diagonals, give the eight possible rows of three. Now surround this matrix of holes with a boundary of crosses (shown here as plus signs). There must plainly be 16 crosses, that is $5^2 - 3^2 = 25 - 9$. Then, through any particular cross, say the cross in the first column and second row, one and only one line can be drawn which passes through three holes. Moreover, this line will pass through one and only one other cross. This is true for each of the crosses. It follows that the number of rows-of-three for the holes of the original matrix is $\frac{1}{2}(5^2 - 3^2) = 8$ as we already know. In exactly the same way in the three-dimensional game Plato, the 27 holes can be surrounded by a boundary of $(5^3 - 3^3) = 98$ crosses, and precisely the same argument establishes that the number of rows-of-three which can be achieved with the 27 holes is $\frac{1}{2}(5^3 - 3^3) = 49$. Moreover, the argument can be extended to give $\frac{1}{2}\{(k + 2)^n - k^n\}$ for the number of rows of k in an n-dimensional k-hypercube. When $k = 4$ which is another well known form of the game, there are 76 rows of four where $n = 3$.

```
+ + + + +
+ o o o +
+ o o o +
+ o o o +
+ + + + +
```

Figure 4

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

WHAT DO YOU DO FOR A LIVING?
MATHEMATICS
I WAS NEVER ANY GOOD AT MATHEMATICS
OH WELL, IT'S NOT UNUSUAL. WHAT DO YOU DO?
I'M A POET
AH, THERE YOU ARE. I NEVER COULD UNDERSTAND POETRY
PEASANT!

Reprinted from *Manifold*, No.15 (1973).
(Student Mathematical Journal,
University of Warwick.)

TOO EMBARRASSED TO ASK ?

G.A. Watterson, Monash University

In its work, the Australian Bureau of Statistics has to ask people some very embarrassing questions. Naturally it wants correct answers, but it may not get them. (Headmaster: "Do you smoke in the school toilet?" Student: "Oh! No, sir!")

Some years ago, a very clever way of overcoming this problem was found. The interviewer gives the interviewee the possibility of *two* questions to answer, the embarrassing one and another, innocuous one. "I want you to answer, truthfully, one of these two questions; (1), Do you smoke in the school toilet? or (2), Is your birthday on an even day of the month? Decide which question to answer by tossing this coin; I will not know which you have answered." This interviewee can now answer "Yes" without embarrassment; he *may* be answering the second question.

The idea behind this type of interviewing is to find out what proportion in the population would answer "Yes" to the first question, if answering truthfully. Call that proportion p_1. We are not really interested in the proportion, p_2, who would answer "Yes" to the second question, because we can calculate it for ourselves. In fact, if birthdays are evenly distributed throughout the year of 365 or 366 days, then as there are 179 "even" dates in the year, $p_2 = \frac{179 \times 4}{3 \times 365 + 366} \approx 0{\cdot}49$. Even if birthdays are not evenly distributed, we may know that $p_2 \approx 0{\cdot}49$ anyhow, from other data. But by giving the person the chance of either answering question (1) or question (2), equally likely, the probability of him answering "Yes" is

$$\tfrac{1}{2} \times p_1 + \tfrac{1}{2} \times p_2, = p \text{ say,}$$

using the "Law of Total Probability".

We can estimate p by doing a large sample survey of the population. We can then estimate the sought-after proportion p_1 by

$$p_1 = 2p - p_2,$$

even though nobody but the interviewees knows which questions they were actually answering.

Suppose that 30 boys out of 100 answered "Yes". This would suggest that the proportion who smoked in the toilet was approximately

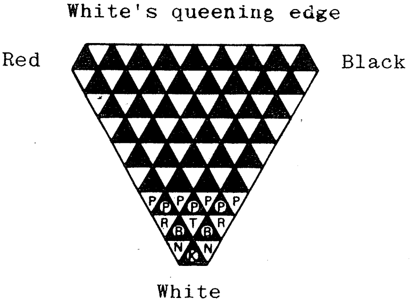
$$p_1 = 2 \times \frac{30}{100} - 0{\cdot}49 = 0{\cdot}11,$$

but not one of them has incriminated himself!

LETTERS TO THE EDITOR

TRIANGULAR CHESS

I have spent some considerable time trying to invent a variation of chess for three players. After a lot of failures, I've come up finally with a playable game. The board is triangular, with triangular spaces (97 of them: 52 white and 45 black). There are three "armies" (White, Black and Red), each of 15 pieces: one King, two Rooks, two Bishops, two Knights, seven Pawns and one Trois. This last is a new piece, so called because it can move in any direction up to three triangles. There is no Queen initially, but if a pawn reaches the opposite edge, the Trois is promoted to Queen power - i.e. its range becomes unlimited. The first Pawn to reach the opposite edge is removed from the board, but subsequent Pawns are promoted to Queens.



I've played this game with my two sons and feel seriously enough about it to have taken steps to secure copyright and patent cover. Of course there's much more than I can go into here - precise move rules, etc., but this may give some idea of my invention.

Roley Whiting,
10/3 Condamine Court,
Turner, A.C.T.

A FACETIOUS APPLICATION OF THE FIBONACCI SEQUENCE

The *Fibonacci Sequence* (see *Function, Vol.1, Part* 1) is

1 1 2 3 5 8 13 21 34 55 89 etc.

After the first two numbers, successive entries are calculated by adding together the two preceding numbers. We may write the sequence out twice as follows:

1 1 2 3 5 8 13 21 34 55 89 etc.
1 2 3 5 8 13 21 34 55 89 144 etc.

In this form, it gives a fairly accurate table for converting miles to kilometres, or *vice versa*. E.g. 8 miles $\simeq$ 13 km, or 89 km $\simeq$ 55 miles. We may interpolate easily. Suppose we want the kilometric equivalent of 28 miles. Then $28 = 21 + 5 + 2$. This converts to $34 + 8 + 3$ - i.e. 45 km, which is the correct answer to the nearest integer. Conversely, 73 kilometres $(2 \times 34 + 5) \approx 45$ miles $(2 \times 21 + 3)$.

The reason for this is that successive terms of the Fibonacci sequence, $f_0 = 1$, $f_1 = 1$, $f_2 = 2$, $f_3 = 3$,$f_4 = 5$, $f_5 = 8$, etc., satisfy the relation

$$\frac{f_{n+1}}{f_n} \to \frac{1+\sqrt{5}}{2} \simeq 1{\cdot}618.$$

The number of kilometres to a mile is approximately $1{\cdot}609$, so the approximation is quite good.

R.R. Watson,
Melbourne High School.

[For more on the miles to kilometres question, see Problem 3.5.4. Eds.]

THE APPLEFORD APPROXIMATION

Suppose we write out a table of functions and their anti-derivatives (ignoring the constant):

$f(x)$	x^{-2}	$x^{-1\cdot1}$	$x^{-1\cdot01}$	$x^{-1\cdot001}$	x^{-1}	$x^{-0\cdot999}$	$x^{-0\cdot99}$	$x^{-0\cdot9}$	x^{0}
$F(x)$	$-x^{-1}$	$-10x^{-0\cdot1}$	$-100x^{-0\cdot01}$	$-1000x^{-0\cdot001}$	$\log_e x$	$1000x^{0\cdot001}$	$100x^{0\cdot01}$	$10x^{0\cdot1}$	x^{1} .

This pattern suggests the following approximation

$$\log_e x \simeq \lim_{n\to\infty} \frac{n}{2}\left(x^{1/n} - x^{-1/n}\right) = y \text{ (say)}, \qquad (1)$$

found by averaging the values on either side of $\log_e x$ in the table. The approximation could also be written, putting $n = 1/t$,

$$\log_e x \simeq \lim_{t\to0} \frac{1}{2t}\left(x^{t} - x^{-t}\right) = y \qquad (2)$$

Note that

$$\frac{dy}{dx} = \lim_{t\to0} \frac{1}{2t}\left(tx^{t-1} + tx^{-t-1}\right)$$

$$= \lim_{t\to0} x^{t-1} = x^{-1},$$

which supplies a check on the formula.

David Appleford, Year 12,
Fairhills H.S., Knoxfield.

[David's limiting equations (1) and (2) are in fact exact, but unless x is near 1, we require very large values of n (small values of t) to get good approximations from them. The error involved in the approximation is itself approximated by

$t^2(\log_e x)^3/6$, if this quantity is small, i.e. t must be small or $\log_e x$ must be small, that is to say x must be near 1.

David's use of differentiation to check his formula is correct, though, in strict logic, it requires the theorem

$$\lim_{t\to 0} \frac{d}{dx} f(x,t) = \frac{d}{dx} \lim_{t\to 0} f(x,t).$$

That is to say: the order in which the limiting and differentiation processes are carried out is irrelevant. In the present instance, this is correct, although in other more complicated cases, this is not always true.]

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ Eds.

GRAPHICAL SOLUTIONS OF QUADRATICS

A quadratic equation, $x^2 - ax + b = 0$, can be solved using a circular graph. First plot a point C at (0,1), and then plot (a,b). The line from C to (a,b) may be taken as the diameter of a circle. Find the intersections of this circle with the x-axis. These give the solutions of the quadratic equation.

This works because of the following analysis.

The circle formed has centre point $\left(\frac{a}{2}, \frac{b+1}{2}\right)$. The radius is $\frac{1}{2}\sqrt{a^2 + (b-1)^2}$, by the Pythagorean formula. Thus the equation of the circle is

$$\left(x - \frac{a}{2}\right)^2 + \left(y - \frac{b+1}{2}\right)^2 = \tfrac{1}{4}\{a^2 + (b-1)^2\}.$$

When $y = 0$,

$$\left(x - \frac{a}{2}\right)^2 + \left(- \frac{b+1}{2}\right)^2 = \tfrac{1}{4}\{a^2 + (b-1)^2\} .$$

Multiplying by 4 and expanding, we find

$$4x^2 - 4ax + a^2 + (b+1)^2 = a^2 + (b-1)^2,$$

which simplifies to

$$x^2 - ax + b = 0.$$

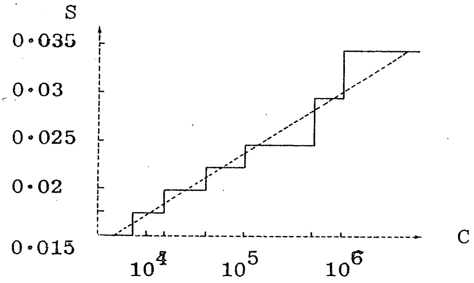
As can be seen, this is the original quadratic, so that its roots are the intersections of the circle with the x-axis.

Janet Watterson, Year 10,
Presbyterian Ladies College.

[It's nice to see this method again. I recall its being on the Year 10 syllabus in Tasmania some 25 years ago, although even then not much attention was paid to it. I liked it because it saved me from plotting parabolas, which I couldn't do very well. M.D.]

MAKING STAMP DUTY FAIRER

Stamp duty is a tax payable to the State on sale of real estate. Let C be the cost of the property and S the rate at which stamp duty is levied. S is a function of C which is represented graphically at the right (solid lines). Note that the horizontal axis is logarithmic (distances are proportional to the difference between the logarithms of the numbers). On this scale, the vertical axis is infinitely far to the left, but has been moved to its present position for convenience.



The method of calculation is irrational, irregular and discontinuous. At each of six arbitrarily selected and rigidly fixed points, the amount payable leaps abruptly and alarmingly, merely because the price increases over the limits by as little as one dollar. In one case, the extra tax on this last dollar is a staggering $5003.50!

If the price lies at the foot of a precipice, the purchaser gains and the revenue suffers, but if it sits at the left-hand edge of a plateau, the reverse is the case. I suggest the use of the dotted line in place of the present formula. This has been chosen to make the total area of the six triangles to the left equal to that of those to the right.

A relatively straightforward calculation gives the result

$$S = \left(\frac{\log C - \log 1075}{\log 32} + 1.1\right)/100,$$

where the logarithms are taken to base 10.

George Strugnell, Solicitor,
106 Bell Street, Coburg.

[There certainly seems to be some merit in Mr Strugnell's suggestion. His formula may be given to reasonable accuracy as

$$S = \left(\frac{2}{3}\log C - 1\right)/100.$$

It would be nice to think our legislators were progressive enough to adopt some such suggestion. Eds.]

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

QUICKIE PROBLEM

If an outward journey is undertaken at 20 k.p.h. and the return journey at 30 k.p.h., what is the average speed?

Submitted by J.F. Pike,
Rydalmere, N.S.W.

PROBLEM SECTION

COMPLETED SOLUTION TO PROBLEM 3.1.2

We require four consecutive odd numbers whose product is a square. It may readily be seen that there are three cases.
(1) The numbers are -3,-1,1,3. This gives a solution.
(2) All the numbers are positive. We consider this case below.
(3) All the numbers are negative. This reduces to Case 2.

Consider now Case 2. Let the numbers be $2n - 3$, $2n - 1$, $2n + 1$, $2n + 3$, where $n \geqslant 2$. Then

$$(4n^2 - 9)(4n^2 - 1) = m^2 \text{ (say).}$$

This gives $4n^2 = 5 \pm \sqrt{m^2 + 16}$, so we require $m^2 + 16$ to be a perfect square. There is only one such case, given by $m = 3$. Then $4n^2 = 0$ or 10, both of which are inadmissible. Hence the only solution is that given by Case 1.

SOLUTION TO PROBLEM 3.2.2

$P(x), Q(x), R(x)$ are all polynomials and satisfy the identity

$$P(x^3) + xQ(x^3) = (1 + x + x^2)R(x).$$

Prove that $P(x), Q(x), R(x)$ are all divisible by $x - 1$.

No one solved this problem, which was based on a U.S. Math. Olympiad question. The key to one method of solution is to be found in Hans Lausch's article on Galois (*Function*, Vol.3, Part 2). There are three cube roots of 1, namely 1 itself and the two complex numbers $\omega = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$, $\omega^2 = -\frac{1}{2} - \frac{i\sqrt{3}}{2}$. Substitute these into the identity to get three equations:

$$\begin{aligned} P(1) + Q(1) &= 3R(1) \\ \left.\begin{aligned} P(1) + \omega Q(1) &= 0 \\ P(1) + \omega^2 Q(1) &= 0 \end{aligned}\right\} & \quad (\text{as } 1 + \omega + \omega^2 = 0). \end{aligned}$$

Solve these to find $P(1) = Q(1) = R(1) = 0$.

Hence $P(x), Q(x), R(x)$ are all divisible by $x - 1$, by the remainder theorem.

SOLUTION TO PROBLEM 3.2.3

This problem asked for a proof that, of all the teenagers in the world, at least two had the same number of teenage friends.

Let us agree on two usages:

(1) We will not allow the case "*A* is a friend of *A*";

(2) Assume that "*A* is a friend of *B*" implies "*B* is a friend of *A*".

Then if there are n teenagers, each may have m friends, where

$$m = 0 \text{ or } 1 \text{ or } 2 \text{ or } \ldots \text{ or } (n - 1).$$

If the result is to be false, then m must take each of these values exactly once, as there are precisely n such values. But, then, one teenager has all the others as friends while another is totally friendless. This contradicts statement (2) and so the result is proved.

SOLUTION TO PROBLEM 3.2.4

The problem read:

A bag contains three red balls and five white ones. Balls are drawn at random from the bag without replacement, until all have been withdrawn. Show that the probability of getting a red ball on *any* particular draw (e.g. the fifth) is 3/8.

Suppose that after a number of draws, m red and n white balls remain. The probability of drawing a red ball is $m/(m + n)$. On the next draw, we will have either

$(m - 1)$ red balls and n white ones, with probability $m/(m + n)$
or m red balls and $(n - 1)$ white ones, with probability $n/(m + n)$.

Thus our chance of drawing a red ball this time is

$$\left(\frac{m - 1}{m + n - 1}\right)\left(\frac{m}{m + n}\right) + \left(\frac{m}{m + n - 1}\right)\left(\frac{n}{m + n}\right) = \frac{m}{m + n} .$$

Thus the probability is the same from draw to draw. As it was initially 3/8, this is the value for all draws. It is important to realise that this probability is that which we assign *before* any balls are drawn. It should not be confused with the conditional probability, given some later information.

SOLUTION TO PROBLEM 3.2.7

Given real numbers a, b, c, the problem was to prove that

$$3a^2 + 4b^2 + 18c^2 - 4ab - 12ac = 0 \qquad (*)$$

implied $a = 2b = 3c$.

Equation (*) may be written

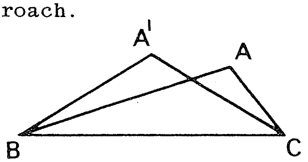
$$(a - 2b)^2 + 2(a - 3c)^2 = 0.$$

But squares are never negative, hence each is zero, and the result follows.

SOLUTION TO PROBLEM 3.2.8

We are given (say) a loop of string of length ℓ and are asked to arrange it as a triangle. Prove that this triangle has maximal area if it is equilateral.

A number of calculus proofs are possible, but most become very tedious. Here is a simpler approach. Let ABC be the triangle giving the maximal area. Suppose it is not equilateral. Then some vertex, say A, connects sides which are unequal. Keep B,C fixed, but move A to A' where $A'B = A'C = \frac{1}{2}(AB + AC)$. Clearly this increases the height of the triangle while leaving the base unaltered. We have thus increased the area, contrary to our assumption.



SOLUTION TO PROBLEM 3.3.1

This question asked if it is possible to construct two loaded dice in such a way that the totals 2,3,4,...,12 shown on their uppermost faces after a toss are all equiprobable.

The answer is "no". For suppose the first dice to be loaded so that the probabilities of 1,2,3, etc. falling uppermost are p_1, p_2, p_3, etc.($p_1 + p_2 + \ldots + p_6 = 1$). Similarly let the probabilities for the second dice be q_1, q_2, q_3, etc. We now have

$$\Pr\{\text{total} = 2\} = p_1 q_1 = \frac{1}{11} \qquad (1)$$

$$\Pr\{\text{total} = 7\} = p_1 q_6 + p_2 q_5 + \ldots + p_6 q_1 = \frac{1}{11} \qquad (2)$$

$$\Pr\{\text{total} = 12\} = p_6 q_6 = \frac{1}{11} \qquad (3)$$

along with eight other similar equations.

But now, by Equations (1), (2), $q_6 \leqslant q_1$, $p_6 \leqslant p_1$, while Equations (2), (3) imply $q_6 \geqslant q_1$, $p_6 \geqslant p_1$. This means that $p_1 = p_6$ and $q_1 = q_6$, but now Equation (2) reads

$$p_1 q_1 + p_2 q_5 + \ldots + p_1 q_1 = \frac{1}{11},$$

contradicting Equation (1).

SOLUTION TO PROBLEM 3.3.3

The problem was to devise a method for multiplying two four-figure numbers together, using trigonometric tables (rather than logarithms).

There are several possible techniques, of which this may be the simplest. Begin with the formula

$$\cos A \cos B = \tfrac{1}{2}[\cos(A - B) + \cos(A + B)]$$

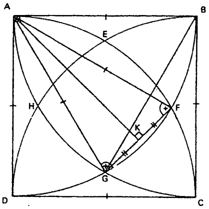
and treat the numbers as cosines of angles. E.g. to multiply

0·1357 by 0·8249, note that these numbers are respectively cos 82° 12' and cos 34° 24' (to the nearest minute). Then their product is ½[cos 47°48' + cos 116° 36'] = ½[cos 47° 48' - cos 63° 24'] = ½[0·6717 - 0·4478] = 0·1120. This may be compared with the true answer of 0·1119.

Decimal points in other positions are best dealt with by adjusting the calculation, using powers of 10.

SOLUTION TO PROBLEM 3.3.4

Lindsay Pope of Motueka H.S. (N.Z.) asked for the area *EFGH* enclosed between the four quadrants inscribed in a square *ABCD*, whose side we will call a.



A calculus approach gives the answer, but David Lumsden (4th Form, Scotch College) and Paul Burnett (Form 5, Boronia Technical School) both sent accounts of a nice geometric solution. We print a composite of their letters.

Construct the triangles *AFG*, *BAG*. This latter is seen to be equilateral, so that $\angle BAG = \pi/3$. Similarly $\angle DAF = \pi/3$, and it follows that $\angle FAG = \frac{\pi}{6}$. Then because the triangle *FAG* is isosceles, $\angle AFG = \angle AGF = \frac{5\pi}{12}$. Note that $AF = AG = a$.

Now the area required is equal to the sum of the area of the *square EFGH* and four times the area of the minor segment on the chord *GH*. To find this latter area, compute the area of the *sector AFG*. This is readily seen to be $\pi a^2/12$. We now subtract the area of the *triangle AFG* which is $\frac{1}{2}a^2 \sin\frac{\pi}{6}$, that is to say $a^2/4$. Thus the segment area is $(\pi - 3)a^2/12$, and the area required is

$$\overline{GF}^2 + (\pi - 3)a^2/3 = 4a^2 \cos^2\frac{5\pi}{12} + (\pi - 3)a^2/3$$

$$= a^2(4\cos^2\frac{5\pi}{12} + \frac{\pi}{3} - 1) \simeq 0\cdot315a^2,$$

which may also be expressed as

$$2a^2(2\sin^2\frac{\pi}{12} + \frac{\pi}{6} - \sin\frac{\pi}{6}).$$

This allows us to arrive at the form given by the proposer, namely $a^2(1 - \sqrt{3} + \frac{\pi}{3})$.

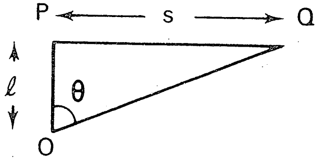
A few new problems for the vacation period follow.

PROBLEM 3.5.1

Mr Ray Bence, formerly deputy curator of Carlton Football Ground, noticed that some football scores may be calculated correctly by multiplying the number of goals by the number of behinds. He asks for a list of all scores for which this is possible. (For those in our northern states, or not up with Australian Rules, the score is calculated by adding the number of behinds to six times the number of goals.)

PROBLEM 3.5.2

This is based on a problem from Fitzpatrick and Galbraith's *Applied Mathematics*, referred to us by a number of teachers. A camera at O tracks a horse running along *PQ*. We require the value of *s* for which θ is maximised, given that its velocity at *P* is *u*, and that its (uniform) acceleration is *a*.



PROBLEM 3.5.3

(Submitted by Y-T. Yu, Knox Technical School, Boronia.)

Set $s_1(n) = 1 + 2 + 3 + \ldots + n,$

$$s_2(n) = 1^2 + 2^2 + 3^2 + \ldots + n^2,$$

$$s_3(n) = 1^3 + 2^3 + 3^3 + \ldots + n^3.$$

When does n divide $s_1(n)$? $s_2(n)$? $s_3(n)$? Can the result be generalised?

PROBLEM 3.5.4

The number of kilometres in a mile is often given as $\frac{8}{5}$. Given *only* that the approximation is expressed *in this form*, estimate the error involved.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

THE VALUE OF SYMMETRY CHECKS

News of the safari racket surfaced when hunters noticed that one lion had made four left-paw prints.

The Age, 7.9.1979.

THE THEOREM THEOREM

If if, then then.

Journal of Irreproducible Results, Vol.25 (1979).

ODD ODDS

Recently, *The Age* (21, 22, 23, 24/8/'79) gave some space to the problem of computing the odds that four consecutive numbers occur in a Tattslotto draw. That is to say: Of the numbers 1,2,3,...,40, six are chosen at random. What is the probability that four (or more) of these are consecutive? Published answers varied from 1/174 to 1/3·8 million.

Dr G.A. Watterson (one of *Function*'s editors) and some others got the right answer. The reasoning is as follows. There are $\binom{40}{6}$ ways of completing the draw. If exactly four of these are to be consecutive, then we could have:

(a) 1,2,3,4, not 5, and two of the remaining 35 numbers.

(b) 40,39,38,37, not 36, and two of the remaining 35 numbers.

(c) 2,3,4,5, not 1 or 6, and two of the remaining 34 numbers.

(d) Similar cases to the last beginning the consecutive run with 3,4,5,...,36.

The number of ways in which Case (a) can occur is $\binom{35}{2}$. Similarly for Case (b). Case (c) can occur in $\binom{34}{2}$ ways, as can each of the 34 Cases (d). This gives a total of

$$2\binom{35}{2} + 35\binom{34}{2} = 20825 \text{ ways}$$

out of

$$\binom{40}{6} = 3838380 \text{ in all.}$$

Taking the ratio of these two numbers gives 0·00543 or 1/184. The odds against exactly four consecutive numbers are thus 183 to one.

For five consecutive numbers, we have (computing as above)

$$2 \times 34 + 34 \times 33 = 1190$$

possibilities, and for six consecutive numbers we have exactly 35 possibilities. This gives a total of 22050 draws having four or more consecutive numbers. This corresponds to a probability of 22050/3838380, i.e. 0·00574 or 1/174. The odds are thus 173 to one against.

Slightly different interpretations (e.g. counting five consecutive numbers as two consecutive groups of four, etc.) can give slightly different answers.

Dr Watterson notes that of the first 360 Tattslotto draws, six in fact did produce results of the type under discussion. The probability of six or more such results out of 360 may be calculated, from the Poisson distribution, as

$$1 - e^{-\mu}(1 + \mu + \mu^2/2 + \dots + \mu^5/5!),$$

where $\mu(= 0{\cdot}00574 \times 360)$ is the expected number of such results.

This gives $\mu = 2{\cdot}07$ and a probability of approximately 0·02.

The probability of such a result occurring purely by chance is thus 1/50, which is food for thought.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

A LARGE SLICE OF PI

Tokyo: Hideaki Tomoyori, 46, an electronics company worker, yesterday claimed a world record by memorizing 15 151 decimal places of "pi", the ratio of the circumference of a circle to its diameter.

He recited that number of digits after the decimal point correctly to three newsmen at the Yomiuri newspaper company here in three hours and ten minutes, breaking the world record of 5 050 set by Michael John Poultney in England in March, 1977, and recognized by the Guinness Book of Records.

Tomoyori, who works for the Sony Corp., was inspired to the feat when a 17-year-old Canadian student memorized the ratio down to the 8750th decimal place last August. The student's record has yet to be endorsed by Guinness.

A resident of Yokohama, Tomoyori adopted the method of memorizing figures in groups of ten and translating them into phonetic approximations to words.

For example, the figures "2,9,8" could be pronounced "fu,ku, ya" in Japanese and be remembered as Fukuya, which means "tailor".

After every 100 places, he bent fingers on his right hand and after every ten places, those of his left hand in associated motions to remember figures.

Tomoyori recited digits with a break after every 1000 places while the newsmen checked them with computer readouts of pi.

From a recent report in the San Francisco Chronicle.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

THE HAWKINS CIPHER

Professor Crossley's letter (*Function*, Vol.3, Part 4) deals with an interesting detective story in the history of mathematics. The "strange message" reproduced is written in code - a rather simple code. To read it, adopt the following rules:

(a) Interchange the following pairs of consonants (*b*,*z*), (*c*,*x*), (*d*,*w*), (*f*,*t*), (*g*,*s*), (*h*,*r*), (*l*,*p*), (*m*,*n*);

(b) Delete vowels indicated by a grave accent (*è*,*ò*).

The message then appears as a letter reading:

Amico suo Amantissimo Johanni Perkes *Ptochotrophii Fohliensis In Comitatu Wigorniensi Ludimagistro*

SIR,

If you Pleas to bestow some of your spare hours in perusing the following treatise you will then be the better able to judg how I have spent mine, and if my paines therein may be Profitable to the publick I have my wish, but if not, it is not a good thing now indeed I do say so.

SIR, I am
Your humble servant
John Hawkins.

Octob. 30. 1684.
From London

The opening lines are in Latin and translate as: *To his very dear friend* John Perkes (= modern Parkes) *of Folie's* (= Foley's) *poorhouse in comradeship to the Worcester schoolmaster*. Presumably, John Parkes, the Worcester schoolmaster, taught at Foley's poorhouse.

The cipher has an interesting structure. Of the 26 letters of the alphabet, 8 are regarded as vowels (*a*,*e*,*i*,*o*,*u* and also *y*, *j* (regarded as a variant of *i*), and *v* which is looked on as a variant of *u*). The remaining 18 consonants are written out in the pattern at right (known technically as symmetric boustrophedon). The interchanges appear when the letters are paired vertically. (There is one exception: *k*, *q* do not interchange, presumably because *q* is always followed by *u*.)

b	*c*	*d*	*f*	*g*	*h*	*k*	*l*	*m*
z	*x*	*w*	*t*	*s*	*r*	*q*	*p*	*n*

It is more difficult to discern why the extra vowels, *è*,*∂* were inserted. Most probably they separate certain unpronounceable combinations of consonants in the coded version.

The reason for the cipher was discussed by de Morgan (1806 - 1871) in an article in the *Penny Cyclopedia* (1838). Cocker was a highly popular and successful author, who was in fact dead in 1684. The suggestion is that Hawkins actually wrote the *Decimal Arithmetick*, but appended Cocker's name to it to increase sales. The letter is seen by de Morgan as a veiled confession of authorship.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

THE SCIENCE MAGAZINE

Function's sister magazine from Monash - *The Science Magazine* - has sent out two free issues this year. The editors are Drs Ann Lawrie, Ian Rae and Keith Thompson from the Science Faculty. If you would like to receive copies, write to the editors (c/- Science Faculty, Monash University). Next year, there will be three issues, which will be sold. Subscriptions are $4.00 per annum and should be mailed to Dr Rae.

Articles have so far appeared on the whale oil versus jojoba bean debate, mercury in the environment, the Omega navigation system, hydrogen at Harrisburg and other topics.