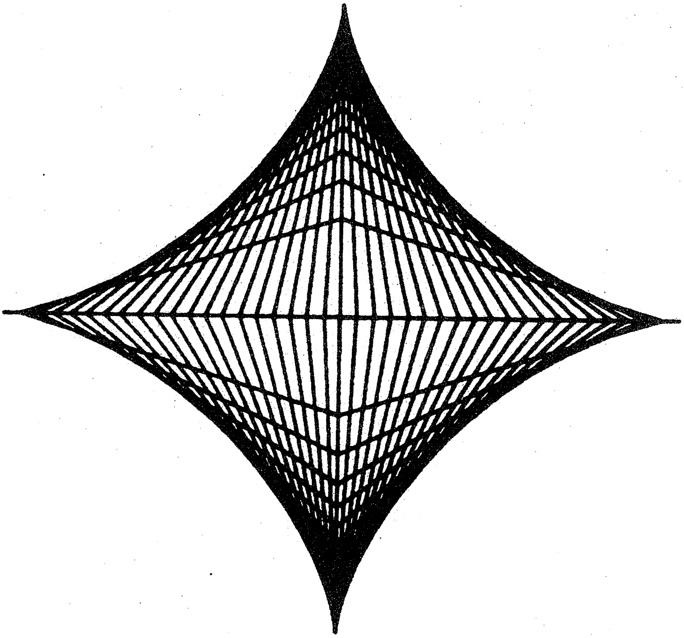
ISSN 0313-6825

FUNCTION

Volume 2 Part 4

August 1978



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.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

EDITORS: G.B. Preston (chairman), N.S. Barnett, N. Cameron, M.A.B. Deakin, B.J. Milne, J.O. Murphy, G.A. Watterson, (all at Monash University); N.H. Williams (University of Queensland); D.A. Holton (University of Melbourne); E.A. Sonenberg (R.A.A.F. Academy); K.McR. Evans (Scotch College, Melbourne)

BUSINESS MANAGER: Joan Williams (Tel. No. (03) 541 0811, Ext.2591)

ART WORK: Jean Hoyle

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): $3.50; single issues 90 cents. 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"

We have given pride of place this issue to the winning essay in a competition for second form students held some weeks ago. More information about the competition and about a poster competition that was held at about the same time is in the article *Maths is Fun for Everyone* that follows it.

The hand calculator, as also the electronic computer, is an immense aid to mathematics. Some hand calculators today have more calculating power, for special purposes, than the first electronic computer; and today's desk computers are generally more powerful than the first large computers of the early 1950's. Computation gives the opportunity to investigate the behaviour of functions which defy attempts to understand them theoretically. On the other hand it is always important to understand the tools one uses: our article *The Accursed Calculator* emphasizes some of the pitfalls open to the unwary user of a hand calculator.

CONTENTS

THE FRONT COVER
J.O. Murphy, Monash University

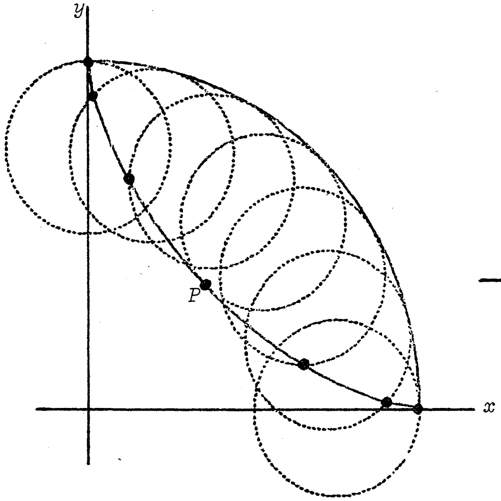
The astroid, with equation $x^{\frac{2}{3}} + y^{\frac{2}{3}} = a^{\frac{2}{3}}$, is the solution to the problem - find the curve such that the length cut off its tangent by the coordinate axes is a constant, say a. Over the last two centuries this curve seems to have been known under a variety of names such as the cubocycloid, four-cusp-curve and now generally as astroid. On the front cover it is generated as the envelope of a line, length a, sliding with its ends in contact with the x and y axes. The actual construction represents the situation of a ladder, for example, with its base resting on a horizontal surface, initially placed against a vertical wall, and then sliding with constant horizontal velocity outwards from the wall with the upper end remaining in contact with the wall. Each line as drawn represents the position of the ladder at equal intervals of time from the commencement of sliding.

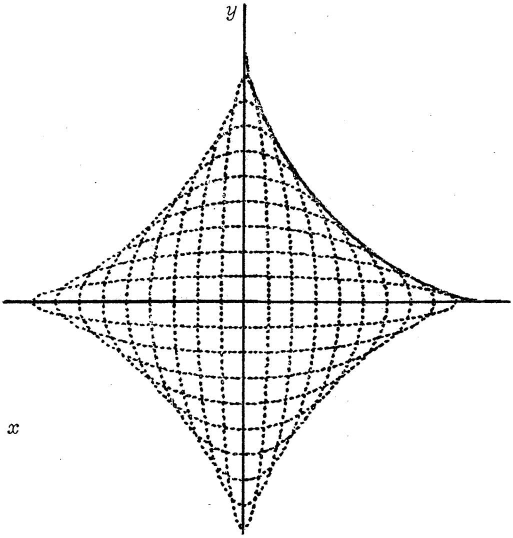
The four segments of the curve can also be represented by

$$x = a \cos^3 t, \quad y = a \sin^3 t$$

and they enclose an area $A = \frac{3}{8}\pi a^2$, where a represents the radius of the circumscribed circle or an area $\frac{3}{2}$ times that of the inscribed circle.

The astroid is also the hypercycloid formed by a circle of radius $\frac{a}{4}$ rolling inside one of radius a; in the diagram below, it is the locus of a point P on the circumference of the rolling circle. In the other diagram a sequence of ellipses, each having a common centre at the origin and defined such that the sum of the major and minor axes is constant, envelopes the astroid curve.





WHY SHOULD GIRLS DO MATHS?

WINNING ESSAY IN COMPETITION FOR SECOND-FORM STUDENTS

Catherine Nichols, Form 8H, Presbyterian Ladies College, Melbourne

Why should girls be denied the excitement of maths?

It is in fact an extremely exciting subject. There is the challenge of even some of the simplest problems, the thrill and the pleasure you get when you find out what x is equal to, or when points on a graph fall into place and you suddenly realise what is going on.

There is also the lovely feeling when you look at a maths sheet and can understand and do what it is asking you to.

Secondly, I object to the ... question.

I think that there should be no difference between the subjects that girls do and the subjects that boys do. Maths should not be a subject that one sex does and the other not.

Girls' brains are no less able than boys' brains so they can do maths just as easily as boys can.

Boys should learn more subjects like Domestic Science, sewing, etc., which would prepare them better for living.

Girls should be able to do whatever jobs they would like to. We should be able to be engineers or mechanics if that is what we would like to be.

We shouldn't have to do only jobs that are labelled "Girls' jobs".

We should do whatever we are best suited to and would like.

Learning maths enables us to do lots of things when we leave school.

For many jobs and courses it is required that you have done maths at school. Maths is also useful in your day-to-day living - for instance the adding up of bills and accounts.

We are living in a very technical age - more and more advances are being made into science etc.

Girls (women as well) are approximately 50% of the population.

Maths are needed for so many fields that it seems wasteful that girls should not be taught how to make proper use of their brains to help the world.

* * * *

MATHS IS FUN FOR EVERYONE

...was the title of a poster competition recently conducted under the auspices of the Australian College of Education. This competition was for grade five pupils and an essay competition for second-form (i.e. year eight) students was also held, the essay title being "Should Girls do Mathematics?"

About 450 essays and 400 posters were received and the winning essay, from Catherine Nichols at Presbyterian Ladies' College, Burwood, is reproduced overleaf.

In mathematics learning, motivation is of great importance. It is clear that from late primary years boys are motivated and encouraged to pursue mathematics for career purposes, and girls are not. A group of concerned teachers and others has been formed to help foster knowledge of the careers now open to girls for which mathematics is a prerequisite, and to encourage girls to keep as many options open as possible.

The group has collected names of women willing to act as speakers in schools, particularly to girls in later secondary years who are interested in careers involving mathematics or with a prerequisite of mathematics. Secondary teachers at Metropolitan schools who would be interested in having a visit at their school from one of these speakers, should write to Miss Kaye Marion, Mathematics Department, Royal Melbourne Institute of Technology, mentioning the age and numbers of pupils involved.

Send a large self-addressed envelope with a 25¢ stamp to Dr Susie Groves, Mathematics Department, Burwood State College of Victoria, for a guide to literature on the relevance of mathematics to careers for girls.

Teachers or others interested in becoming involved with this group are invited to contact either Miss Marion, Dr Groves, or Mrs Shirley Sampson, Faculty of Education, Monash University.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

NEWTON'S APPLE TREE

Dr G.A.M. Scott, of the department of Botany at Monash, writes:

"The interesting article by G.C. Smith on Newton's Apple (Vol.2 part 1) did not mention that a cutting descended from the original tree is now established in the Monash University grounds.

The original tree at Woolsthorpe Manor is said to have died in 1814 but, before this happened, grafts were taken from it and established at Belton Manor; from these a number of cuttings were taken and grown at East Malling Research Station where they were brought to fruit and identified as the very old - at least Elizabethan - kitchen variety "Flower of Kent". It was from these trees that the Monash cutting was taken and has been grown into what is now quite a large and vigorous tree."

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

THE ACCURSED-CALCULATOR

D.A. Holton, Melbourne University

Phase 1.

Since 1971 the Department of Mathematics at the University of Melbourne has organised an annual mathematics competition for secondary school students under the auspices of IBM. The competition is divided into a Junior Division, for forms 1 to 4, and a Senior Division, for students in forms 5 and 6. In the Senior Division of this year's competition the following question was asked.

> The number $n!$ is defined to be $n \times (n - 1) \times (n - 2) \times \ldots \times 3 \times 2 \times 1$. Hence $3! = 3 \times 2 \times 1 = 6$ and $10! = 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 3628\ 800$.
>
> When $n!$ is calculated for a particular n, it is found that the last 100 digits are zero. What is the smallest value that n can have?

Pause 1.

Of course you can cheat at this stage and move on to *Phase* 2 and look at a solution of the problem. But this pause is designed for you to go away, pick up pencil and paper, and make your own attempt at a solution.

Take your time. I'll wait for you.

Phase 2.

Take one calculator. I am about to give a solution to the problem, so start concentrating. Take one calculator. Now mine actually has an "$n!$" key. With a little bit of experimenting I find that $69! = 1{\cdot}711\ 224\ 522 \times 10^{98}$. If you don't have an "$n!$" key on your machine you'll be able to get to this number too, but it will take you a little longer. Now when I press the keys for 70! the error sign comes up. This means that 70! is $a \times 10^{b}$ where b is 100 or more.

Eureka! The "n" required by the problem is 70.

Pause 2.

Did you get 70? Do you understand the solution I have just given? If you do could you please explain it to me.

I'll wait while you do some hard explaining.

Phase 3.

The solution provided in *Phase* 2 is wrong, yet it was by a long way the most commonly given solution to the competition problem. A complete misunderstanding of what the calculator's answer means is shown by this common response.

What does $1{\cdot}23 \times 10^1$ mean? Simply $1{\cdot}23 \times 10 = 12{\cdot}3$. What does $1{\cdot}23 \times 10^2$ mean? Simply $1{\cdot}23 \times 100 = 123$. What does $1{\cdot}23 \times 10^6$ mean? Simply 1230 000. So when 69! came up as $1{\cdot}711\ 224\ 522 \times 10^{98}$ it meant 17 112 245 2200...0. The string of zeros is 89 long.

Mistake number one: $1{\cdot}711\ 224\ 522 \times 10^{98}$ does not end in 98 zeros, so 70! is unlikely to end in 100 zeros.

But what does a calculator *really* mean when it gives an answer of $1{\cdot}711\ 224\ 522 \times 10^{98}$ to the 69! computation? What it really means is this. It's really saying "Now look here you guys, that's an awfully difficult calculation. If I could I'd work the whole thing out for you exactly. If I had a display and circuitry that would let me give you a 99 digit answer then I'd give you 69! exactly. But I'm sorry. You only paid $32.15 for me and for that price I can only give you ten digits. So I'm afraid I'll have to do a little approximating. The number $1{\cdot}711\ 224\ 522 \times 10^{98}$ is not *exactly* 69!, but it's the best my poor old integrated circuitry can do".

Mistake number two: a calculator can give only an approximate answer to a calculation like 69!. So even though it looks as if 69! *might* end in 89 zeros it doesn't. The number ending in 89 zeros is only an approximation to 69!.

How many zeros does 69! end up with? Work it out.

Pause 3.

I'm waiting for you to answer the last question. When you've done that you can have another go at the original problem.

Don't cheat! Cover up the rest of this article.

Phase 4.

Let's have a look at a *real* solution to the problem. If $n!$ is going to end up with the final 100 digits all zero, then $n! = a \times 10^{100}$, where a is some integer. But $10 = 2 \times 5$, so $n! = a \times 2^{100} \times 5^{100}$. This means that in the numbers $n, n-1, \ldots, 3, 2, 1$ the numbers 2 and 5 must appear 100 times each as factors. But if 5 appears as a factor in m, say, then 2 will be a factor of either m or $m - 1$. And if 5^2 appears as a factor in m, then 2^2 must occur as a factor of the product of the numbers between m and the next number, smaller than m, in which a factor of 5 appears. A similar thing is true for 5^3 and 2^3. So if $n < 5^4$, we only have to count for 5's. We can forget the 2's.

At this stage let's get a rough idea of how large n will be. In 100! we'll have a 5 factor in 100, 95, 90, 85, 80, 75, 70, 65, 60, 55, 50, 45, 40, 35, 30, 25, 20, 15, 10, and 5. There are 20 terms here, so 100! has a factor of 5^{20} at least. To get 5^{100} then, we need go no further than 500!. So $n \leqslant 500 < 5^4$.

Now let's do the counting of factors more carefully. If $n = 5k$, then a factor of 5 will appear in $n!$ as a contribution from $5k$, $5(k - 1)$, $5(k - 2)$, ..., 5×2 and 5×1. So this gives at least $k = \frac{n}{5}$ factors to the total in $n!$. In general the number of times a factor $5r$ will appear is $\left[\frac{n}{5}\right]$, where the square brackets indicate that we take the whole part (integer part) of $\frac{n}{5}$. But every now and again a number $5r$ is divisible by 25, so an extra factor of 5 creeps in to the tally. An extra factor of 5 therefore appears $\left[\frac{n}{25}\right]$ times, where again the square brackets indicate that we take the integer part of $\frac{n}{25}$. And then another factor creeps in whenever one of the numbers less than or equal to n is divisible by 125. So these numbers give a contribution of $\left[\frac{n}{125}\right]$.

We now know that

$$100 = \left[\frac{n}{5}\right] + \left[\frac{n}{25}\right] + \left[\frac{n}{125}\right] .$$

Let $n = 125s + 25t + 5u + v$, where s, t, u, v are all 0, 1, 2, 3 or 4. Then

$$\begin{aligned} 100 &= \left[\frac{125s + 25t + 5u + v}{5}\right] + \left[\frac{125s + 25t + 5u + v}{25}\right] + \\ &\quad \left[\frac{125s + 25t + 5u + v}{125}\right] \\ &= 25s + 5t + u + 5s + t + s \\ &= 31s + 6t + u. \end{aligned}$$

Now $s = 0, 1, 2, 3$, or 4. Clearly $s \neq 4$ or else we shall not have equality. Further, the largest that $6t + u$ can be is $6 \times 4 + 4 = 28$, so s cannot be 0, 1 or 2. Hence $s = 3$. We thus have

$$100 = 93 + 6t + u,$$

which gives

$$7 = 6t + u.$$

The only solution this has for t, $u = 0, 1, 2, 3$, or 4 is $t = 1 = u$. Hence $n = 125 \times 3 + 25 \times 1 + 5 \times 1 + v$, in order to give 5^{100}. But we want the smallest such n, so $v = 0$. Thus $n = 405$.

Moral: He who calculates is lost.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

The function of a mathematician is to do something, to prove new theorems, to add to mathematics, and not to talk about what he and other mathematicians have done.

G.H. Hardy: *A Mathematician's Apology*, 1941.

THE ELEMENTS OF THAT MATHEMATICAL ART COMMONLY CALLED ALGEBRA

G.C. Smith, Monash University

An aspect of the history of mathematics which is generally neglected is that which traces the manner in which the various branches of mathematics have been taught in the past. We can do this by examining the textbooks that have been used in different periods. In this article I want to give an impression of a seventeenth century algebra book written by John Kersey, and the title of which I have borrowed to serve as the title of this article.

The significance of this text is not that it was particularly successful - this is not the case: it has been described as being too elaborate to meet with great success. But it appeared at the time when the symbolical notation for algebra had just become established, it was a substantial work, and it was in English - in the seventeenth century many texts were published in Latin.

In the sense we understand it in elementary mathematics, algebra is primarily a symbolic language for expressing relations between numbers: of course in recent years algebra has also been concerned with expressing non-numerical relationships - such as $A \subset B$, where A and B are sets. But I am not concerned with these 'modern' aspects of algebra, and I shall use the term 'algebra' in the elementary sense which is exemplified by school algebra texts of the 19th and first half of the 20th centuries. Algebra in this older sense began to develop with the work of the French mathematician Viète, who was working around the late 1500's and early 1600's. In the first 30 years of the 1600's there were a number of writers who developed symbols for many operations - in fact there was a tendency to introduce far too many such symbols, and this made it hard to understand the formulae as so many symbols and notations had to be memorised. What was needed was just a few symbols which would serve to express all the common operations of algebra, and which would be straightforward enough to gain universal acceptance. The work which set the pattern which became accepted was Descartes' *La Géometrie*, which appeared in 1637. In fact Descartes' way of writing algebraic formulae is not quite what we use today - but it is not far from it - and it takes only a few minutes to learn the differences and so be able to read Descartes' algebra with ease. In the years following 1637, other symbols and notations were gradually dropped, and the present notation emerged.

So John Kersey's text which was published in 1673-4 appeared at the time when this situation had occurred, and as one of the earliest instances of a large-scale work in English, it has a certain historical importance. Not a lot seems to be known about John Kersey: he was born in 1616 near Banbury in Oxfordshire, England, and died in London about 1690. He is said to have been highly regarded as a teacher of mathematics and a practical surveyor. We know he taught in Charles Street, opposite the White Lion, near the piazza of Covent Garden. His book was said to be the product of his spare hours of twenty years.

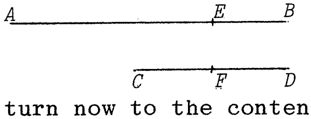
Kersey's book was published in two volumes, volume 1 containing parts 1 and 2 (which he called 'Books 1 and 2'), and volume 2 containing parts 3 and 4. There is also a preface in which the author makes a point of showing that he has done his homework and read all the best works of algebra of the past 170 years or so! The following quotation from this preface will show you the style (and spelling!) of a 17th century work:

> "But the Excellency of the Algebraical Art is best known to those that are aquainted with the most eminent Writers on that Subject; among which these are deservedly Famous namely Diophanties of Alexandria (the first Inventor of this rare Art...) ... Cardano, Tartaglia, Clavius, Stevinus, Vieta (... the happy Restorer of Specious, or Literal Algebra, so called because it operates chiefly by Alphabetical Letters), Mr William Oughtred (our learned Countreyman) whose *Clavis Mathematicae*, for solid matter, neat contractions, and succinct Demonstrations, is hardly to be parallel'd), Mr Thomas Harriot (another learned Mathematician of our Nation), Ghetaldus, Andersonus Bachetus, Heridonus, Cartesius, Fran. van Schooten, ... and many others too numerous to be here recited ... I shall mention four more of our own Nation, and now living ... Seth Lord Bishop of Sarum, Dr John Wallis ..., Dr Isaac Barrow, and Dr John Pell."

So we conclude that Kersey knew most, if not all, of the major writers on algebra up to his time. Notice that Viète, whom I mentioned above, appears with his name Latinised as Vieta - and 'Cartesius' is a Latinised form of Descartes (which in the 17th century was usually written Des Cartes).

Before giving some extracts from the first few chapters I will add one more point about the symbols Kersey uses. The signs > and < for greater and less had been introduced by Harriot in a book published in 1631; however another influential book by Oughtred (which curiously enough was also published in 1631) suggested the signs ⊏ and ⊐ for greater and less, and these were used by Kersey. It was quite some time before > and < became generally accepted. To illustrate his use of these signs, and at the same time show how the influence of Euclid's Elements was still present even in algebra, I will quote Kersey's statement of one of the axioms of Euclid:

> If from unequal quantities equal quantities or one and the same quantity be taken away, the remainders will be unequal.



If $AB \sqsubset CD$ and $EB = FD$
then $AE \sqsubset CF$.

Let us turn now to the contents of Book 1. In those days titles of books, and chapter headings were often very long: they often read like a summary of the book or chapter. Kersey's heading for Chapter 1 is no exception, it reads:

> Concerning the Nature, Scope and Kinds of Algebra. The Construction of Cossick Quantities or Powers; with the manner of expressing them by Alphabetical Letters: The Signification of Characters used in the First Book.

Cossick symbols were an older system of notation for powers - here Kersey is using the old term as a synonym for powers.

The chapter is arranged in numbered paragraphs. Paragraph V gives the aim of algebra:

> V The Scope, Drift or Office of the Analytick or Algebraic Art, is to search out three kinds of Truths *viz.*
>
> 1. Theorems ... This kind of Resolution when it rests in a bare invention of Truth is called Contemplative or Notional.
>
> 2. Canons, or infallible rules to direct how to solve knotty Questions ... this kind of Resolution is called Problematical.
>
> 3. Demonstrations, or ... proofs of such Theorems and Canons.

Notice here the orders in which the three kinds of truths are stated: theorems - which means only the *statements* of the theorems with no proof; then the Canons or rules of calculation; finally the demonstrations i.e. proofs. This way of presenting results was the usual one in the seventeenth century. One first gave the bare statement of the result, in general terms, often in words; then one shows how specific examples are calculated; finally one gives the proof of the general result.

Later in Chapter 1 Kersey explains the use of the addition sign, and the way quantities are designated by letters:

> XX This Character + is a sign of Affirmation, as also of Addition, ... as $+a$ affirms the Quantity denoted by a to be real or greater than nothing ... But when the sign + is placed between two Quantities it imparts as much as the Word plus, or more, and signifies that the Quantities are added...
>
> XXV A simple Quantity is designed or expressed either by a single Letter, or by two or more Letters joyned together like Letters in a Word. As a (or $+a$) is a simple Quantity, likewise $2aa$, $3abc$ and $dddd$ are simple Quantities.
>
> XXVI A Compound Quantity consisteth of two or more simple Quantities connected or joyned one to another by + or -, so $a + b$ is a compound Quantity, likewise $a - c$, also $a + b + c$, and $a + b - c$ are Compound Quantities.
>
> XXVII ... In a like Manner $a - \overline{b + c}$ shows that the Compound Quantity $b + c$ is subtracted ... from the Quantity a.

In these paragraphs notice that in XX Kersey identifies 'greater then nothing' with 'real' - negative numbers were still a mystery at this time. Also in XXV you will have observed $2aa$ and $dddd$: although the raised digit for a power was in use (Descartes used it) many books still wrote powers by repeating the letter an appropriate number of times. Also note in XXVII the use of $\overline{}$ where we would use brackets.

Chapter 2 is about 'Addition of Algebraical Integers'. However this is simpler than it sounds as the following examples will show:

$$\begin{array}{ll|l}
\text{Add,} & \left\{\begin{array}{r}-3b\\ +b\end{array}\right. & \\
\text{Summ} & \overline{-2b} & \\
 & & \\
\text{To be added} & \left\{\begin{array}{l}+ab\\ -ac\\ +ad\end{array}\right. & \begin{array}{r}+5ddd\\ -3dd\\ -4d\end{array} \\ \hline
\text{The Summ} & +ab-ac+ad & +5ddd-3dd-4d
\end{array}$$

Chapter 5 is about division:

IV When the Dividend is equal to the Divisor, the Quotient is 1.

V When the Quotient is expressed Fraction-wise ... if the same Letter or Letters be found equally repeated in every Member of the Numerator and Denominator, cast away those Letters, so the remaining Quantities shall signifie the Quotient. As, for Example, If ab be divided by a, the Quotient expressed Fraction-wise will be $\frac{ab}{a}$, ... I cast away a out of both, so b only is left, which is the Quotient.

If you have been told by some grammatical experts that you should not say fraction-wise as it is an American neologism - you now know they are wrong.

Chapter 10 contains easy problems illustrating the principles that have been explained in the previous chapters: this chapter is titled: Questions to exercise Algebraical Arithmetick.

III There are two Quantities whose difference is d, (or 4) and if for the greater Quantity there be put a, (or 12); What is the lesser? What is their Summ? What is the Product of their Multiplication? What is the Summ of their Squares? What is the difference of their Squares?

1. By subtracting the Difference from the Greater quantity, the Lesser will be	$a-d$	8
2. The Summ of the two Quantities is	$2a-d$	20
3. The Product of their Multiplication is	$aa-da$	96
4. The Summ of their Squares is	$2aa+dd-2da$	208
5. The Difference of their Squares is	$2da-dd$	80

These extracts will give you an impression of Book 1 of Kersey's work - the most elementary part. However later parts of the text do contain results which are at a higher level than these extracts. For example Chapter 11 of Book 2 contains an account of Cardan's method of solving cubic equations.

I will conclude with a quotation from a review of the book, and a reference to it in letters of Newton.

In volume 8 of the Philosophical Transactions of the Royal Society, a review of Kersey's Algebra included the following remarks:

> 'The Author will be found to have so fully and plainly handled the matter, that an ordinary capacity without an other Teacher may attain this excellent knowledg, which extends itself through all the parts of the Mathematicks ... we have this to say from the judgement of sober and knowing Mathematicians, that there is not the like Collection of Algebra extant in Latin or any other Language ...'

Newton thought enough of Kersey to subscribe for a copy before the book was published. In a letter from Newton to Collins of 25 May 1672:

> 'The Coppies of the Synopsis of Mr Kersies Algebra I have communicated to our Mathematicians, but meet not with any subscriptions. However to encourage the undertakings I shall subscribe for one and hope ere long to send you another or two.'

Newton's hope of obtaining further subscriptions was fulfilled. To a letter of 13 July to Collins he wrote a postscript

> 'There are three more of Mr Kersies Bookes of Algebra desired in Cambridge...'

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

TRUNCATION ERROR

A bank teller who worked in New York made his computer rob his own bank and they still do not know how much the pair took. The computer still has its job, the man has not but is free.

The New York bank-robber had a subtle mind and more than a little computer knowledge. He simply told the computer to transfer all the fractions of cents from interest calculations to his private account. He then had the computer pay him and cancel all records of the transaction. Bank officials feel that he got away with between $4-$8 million, but they do not know.

From *Computer crime is growing - and profitable*,
The Weekend Australian Magazine, May 6-7, 1978

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

TOPICS IN THE HISTORY OF STATISTICAL THOUGHT AND PRACTICE
II. RICE, BERI-BERI AND A LUNATIC ASYLUM

Peter D. Finch, Monash University

Beri-beri is a disease which is known to be caused by a deficiency of thiamin (vitamin B1). It used to be prevalent in Japan, China, India, the Phillipines and other countries of Southeast Asia where uncured rather than cured rice was the staple diet. Whereas white uncured rice is cleaned and has its husks removed before use, brownish cured rice is boiled and used unhusked. Since the husk contains the vitamin B1 its removal leads to a diet which produces beri-beri. It was also prevalent during the second world war in Japanese prisoner-of-war camps where the diet was deficient in vitamin B products.

The word 'beri-beri' comes from the Singhalese for 'I cannot' and signifies that the person afflicted feels too ill to do anything. The symptoms include inflammation of the nerves, increasing dropsy of the body, disturbed sensation and loss of muscle power, profound weakness, paralysis and heart disorder. It often results in heart failure and death.

At the beginning of this century the cause of beri-beri was still unknown. A certain Dr Braddon suggested that uncured rice might be to blame but this was only one of several possibilities. Others had suggested that, on the contrary, it was

(1) a place disease, i.e. one peculiar to certain localities,
(2) a parasite disease conveyed by bugs or lice, and
(3) an infectious disease communicated from patient to patient by excreta.

In 1907 Dr William Fletcher, District Surgeon at Kuala Lumpur, published a preliminary report of an experiment conducted at the Kuala Lumpur lunatic asylum. This report appeared on pages 1776-1779 of *The Lancet* for June 29, 1907. This experiment provided the first firm evidence that uncured rice was indeed the cause of beri-beri even though it had been intended to refute rather than confirm Braddon's suggestion. Fletcher admitted that '... at the commencement of the experiment the opinion was held by myself that rice was neither directly nor indirectly the cause of beri-beri. It was fully expected that ... the result of the experiment would be a refutation of the rice theory'.

Fletcher divided the lunatics into two groups of roughly equal size, he then fed one group cured rice, the other uncured rice and, over a period of one year, counted the number of beri-beri cases in both groups. There were 120 lunatics in the group fed uncured rice, 34 of them got beri-beri and 18 of those died from the disease. By way of contrast none of the group fed cured rice went down with beri-beri during the course of the experiment. The message is clear: if the only difference between the two groups was the imposed dietary one then the uncured rice must have been responsible for the beri-beri.

But can one be sure that diet was the only difference between the two groups? If Fletcher had put healthier lunatics in the group fed cured rice, then the observed incidence of beri-beri might be no more than the result of a corresponding discrepancy between the general well-being of the two groups. If the group fed cured rice was located in one place, the group fed uncured rice in another, then what we observe might be a corresponding place effect; this would be consistent with the suggestion that beri-beri is a place disease. If the locality of the group fed uncured rice had been infested by bugs and lice whereas that of the group fed cured rice had not, then the result of the experiment would be consistent with the suggestion that beri-beri is a parasite disease. Even the supposition that beri-beri is an infectious disease communicated by excreta might account for the experimental results if only those in whom mental illness was well advanced had been allocated to the group fed uncured rice and their condition was associated with a marked decrease in personal hygiene.

It is remarkable not only that Fletcher anticipated these objections but also that he took care to design his experiment to take prior account of them. In this experiment he foreshadowed general principles of experimental design which were to be widely recognised only some 20 years later with work of R.A. Fisher.

Prior to Fletcher's experiment the lunatics had only uncured rice. In 1905 an epidemic of beri-beri broke out. It started in February, reached its peak in July and August and declined towards the end of December. Out of 219 lunatics treated in the asylum during 1905, 94 were affected with beri-beri and 27 of them died from the disease. Towards the end of 1905 it was decided to place half the lunatics on cured rice. The experiment started on December 5th, 1905, and continued to December 31st, 1906. Fletcher explained the design in the following way:

> "The lunatics are housed in two exactly similar buildings on opposite sides of a quadrangle surrounded by a high wall. On December 5th all the lunatics at that time in the hospital were drawn up in the dining shed and numbered off from the left. The odd numbers were subsequently domiciled in the ward on the east side of the courtyard and no alteration was made in their diet, they were still supplied with the same uncured rice as in 1905. The even numbers were quartered in the ward on the west of the quadrangle and received the same rations as the occupants of the other ward, with the exception that they were supplied with cured rice instead of the ordinary uncured variety.
>
> At the commencement of the experiment all patients showing unmistakeable symptoms of beri-beri were removed to the district hospital, which is two miles distant from the asylum. On December 5th there were 59 lunatics in the asylum; of these 29 were put on cured rice and 30 on uncured rice. The next patient admitted to the asylum was admitted to the cured rice ward, and the one admitted after him to the uncured rice ward, the next to the cured and so on alternately to the end of the year."

The way in which lunatics were allocated to the two wards effectively reduces the force of the objection that differences between the two groups might be due to factors other than diet. For it is difficult to maintain that selection into the cured rice ward is likely to be biased towards lunatics favoured in some way over their peers, by reason of health, degree of mental illness and so on. It is an early example of randomisation to avoid the possible biasing effect of other factors.

There remains, however, the possibility of a place effect. Fletcher disposed of this possibility in the following way:

> "In view of the theory ... that beri-beri is a place disease, it was thought possible that the east ward was infected. Therefore on June 20th the patients were transposed, those on uncured rice being moved to the west ward and those on cured rice transferred to the east. From June 20th to December 31st no beri-beri developed amongst the patients on cured rice although they were living in a ward where beri-beri had been rife amongst the lunatics who were fed on cured rice."

It was worth noting that this transposition of location also casts doubt on the suggestion that beri-beri is a parasite disease conveyed by bugs or lice.

Further confirmation that uncured rice was the decisive factor was obtained after April. As no patients on cured rice had then developed beri-beri, it was thought that it might benefit those already suffering from the disease to withdraw them from the uncured rice diet and place them on the cured variety. Between April 11 and December 31st 10 cases of beri-beri were transferred in that way, each of them recovered. Moreover, though patients actually suffering from beri-beri were put to live with the lunatics fed on cured rice none of the latter developed the disease. As Fletcher noted, this is opposed both to the theory that beri-beri is a parasite disease and to the suggestion that it is an infectious disease.

Fletcher's experiment is remarkable for the way it anticipated later developments in statistical theory. There was the precise formulation of a null hypothesis to be disproved by the experiment, *viz.* 'that rice was either directly or indirectly the cause of beri-beri', even though it turned out unexpectedly that this hypothesis was confirmed rather than refuted. There was a clear recognition of the importance of randomisation in design to eliminate bias from uncontrolled factors. Finally, by means of the transposition of patients, explicit use was made of variation in experimental conditions to determine if they themselves had any effect on the result. It should also be mentioned that Fletcher was quite aware that he had in no way determined the agency by which beri-beri was contracted. In his concluding remarks he noted that the actual cause could be either a poison contained in the uncured rice or an associated dietary deficiency.

There are important lessons to be learned from this experiment. Not the least of them is a recognition of the role of mathematics in the practice of statistics. Fletcher's result was so extreme that mathematical analysis is not required to unravel its meaning, indeed he could not have got a more extreme result. Yet had it not been so extreme the meaning would not have been so clear. But what would it have meant if there had been a few cases of beri-beri in the group fed on cured rice? The presence of just one such case would have been enough to cast doubt on the supposition that uncured rice was the sole cause of beri-beri. Nevertheless we might have suggested that uncured rice was the predominant factor. Would we say the same if there had been 2 or 3 instances of beri-beri in the group fed on cured rice? What if there had been as many as 10 such cases? It is important to recognise that the mathematical methods of statistics have been developed to unravel the ambiguities of these more general situations. In extreme cases those methods are not required. But where they are required they cannot be divorced from the practical context of experiments like the one discussed here. Careful forethought in design is still required, randomisation is needed to avoid the possibility of bias like that considered earlier and transposition of site still plays a key role in determining whether or not there is a place effect.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

CAN YOU CHECK THE RESULT?

1. Numerical results of mathematical problems can be tested by comparing them to observed numbers, or to a commonsense estimate of observable numbers. As problems arising from practical needs or natural curiosity almost always aim at facts it could be expected that such comparisons with observable facts are seldom omitted. Yet every teacher knows that students achieve incredible things in this respect. Some students are not disturbed at all when they find 16 130 ft for the length of the boat and 8 years, 2 months for the age of the captain who is, by the way, known to be a grandfather. Such neglect of the obvious does not show necessarily stupidity but rather indifference toward artificial problems.

2. Problems "in letters" are susceptible of more, and more interesting, tests than "problems in numbers". For another example, let us consider the frustum of a pyramid with square base. If the side of the lower base is a, the side of the upper base b, and the altitude of the frustum h, we find for the volume

$$\frac{a^2 + ab + b^2}{3}h.$$

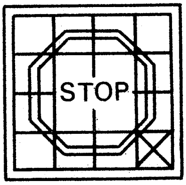
We may test this result by SPECIALIZATION. In fact, if $a = b$ the frustum becomes a prism and the formula yields a^2h; and if $b = 0$ the frustum becomes a pyramid and the formula yields $\frac{a^2h}{3}$. We may apply the TEST BY DIMENSION. In fact, the expression has as dimension the cube of a length. Again, we may test the formula by *variation of the data*. In fact, if any one of the positive quantities a, b or h increases the value of the expression increases.

G. Polya, *How to Solve it*, 1945.

THE 15-PUZZLE, FROM "A LAW OF THE INNER WORLD OF THOUGHT"

Peter A. Watterson, Science II, Monash University

Most people, I'm sure, are familiar with the type of puzzle in which one tries to order certain counters by sliding them about a square. One recent version of the puzzle consists of forming the "STOP" sign from fifteen plastic squares. The sign and its mathematical form are shown below (the cross representing a blank square). It was just on one hundred years ago that Sam Loyd patented this latter form of the puzzle, "The 15 Puzzle". One had to start with the "14" and "15" inverted and find legal moves to correct them. The $1000 offered by Loyd for the first correct solution apparently created great interest for in the 2nd volume of the American Journal of Mathematics, 1879, the editors comment (after articles by Johnson and Story):



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	☒

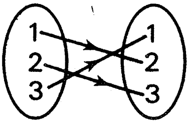
> '"The 15 Puzzle" for the last few weeks has been prominently before the American public, and may safely be said to have engaged the attention of nine out of ten persons of both sexes and of all ages and conditions of the community.'

By the end of this article, the reader should understand why no solution to Loyd's problem is possible, and in fact should be able to determine quickly whether a solution is possible for any given initial and required finishing arrangements for any size rectangular puzzle.

I'll start by introducing the concept of a permutation. A permutation is simply a one-to-one mapping, σ, of the set $\{1,2,\ldots,n\}$ onto itself. It is written

$$\sigma = j_1 j_2 \ldots j_n \text{ where } j_i = \sigma(i).$$

As an example



is abbreviated $\sigma = 231$.

(One observes that there are $n!$ such permutations.)

We say that σ is odd or even according as to whether there is an odd or even number of "inverted" pairs, (i,k), pairs for which $i < k$ but $\sigma(i) > \sigma(k)$. In other words we consider $j_1 j_2 \cdots j_n$ and taking each j in turn, count the number of succeeding j's less than this one. For example in $\sigma = 231$, 2 is not greater than 3 but is greater than 1, and 3 is greater than 1 - two pairs in all, therefore an even permutation.

Now probably the most important property of the even-or-odd-ness, called *parity*, of a permutation is that the interchange of any two numbers acts to change its parity (for example 321 is odd). To show this we only need to consider the numbers located between i and j, the numbers to be interchanged (since the order of pairs formed between i (or j) and "external" numbers will be unaffected. We assume $i < j$ and consider the two cases: (i) i precedes or (ii) i succeeds j in the permutation. Let m of these intervening numbers be less than i, n between i and j, and p greater than j. For case (i), the movement of i changes the number of inverted pairs by $(n + p - m)$, that of j by $(m + n - p)$, and since j now precedes i, the net change is

$$(n + p - m) + (m + n - p) + 1 = 2n + 1.$$

For case (ii), the interchange produces a net change

$$(m - n - p) + (p - m - n) - 1 = - 2n - 1.$$

In both cases the number of inverted pairs changes by an odd number and by the number properties: even + odd = odd, odd + odd = even, the permutation is observed to change its parity.

The 15-Puzzle now yields as a direct application of this theory. Consider any arrangement of the counters in which the blank space is in the lower right hand corner and regard the blank space as a "16". Now this naturally constitutes a permutation between the squares as correctly numbered (on an earlier diagram) and the counters on them. The advantage of regarding the space as "16" is that *any* move now becomes an interchange between counter "16" and some other counter. Also the number of moves taken by "16" in completing any journey ending where it started (at the lower right-hand corner) must be even - since in such a path the "16" must make as many up as down, right as left moves. Finally, since 123...16 is an even permutation (no pairs are inverted), for this to be obtained (by an even number of interchanges) from an initial permutation, this initial permutation must also have been even. Hence Loyd's puzzle, which starts from an odd permutation, can not be solved - which probably explains why the thousands of people who claimed to have performed the feat could never seem to recall their solutions.

The above discussion applies to any rectangular board and says that if a particular arrangement is an odd permutation relative to a particular final solution then the conversion can not be made. (It is always assumed that the initial arrangement has the blank space in the correct position, that of the solution - if not, make any moves to put it there.) For example we can deduce quite quickly that the following arrangement,

4	2	1
5	╳	3

2	5	3
4	╳	1

, can not be converted into , since the relative permutation is σ = 34152, which is odd. [Note: there is no need to repeat the argument which would name the blank space "6" and the permutation σ = 341526 since the final term will (always) be the largest and will have no effect on the parity of the permutation.]

But now we want to go on and prove that any even arrangement can be converted into any other even arrangement, and hence the solution. We can do this by proving that every even arrangement can be converted to a particular even arrangement, and hence, *via* this, to the even solution.

First, we introduce an ordering system which orders the counters starting at the top left corner of the rectangle along the first row, back along the second, along the third, etc., ignoring the blank when it occurs. For example,

4	2	1
5	╳	3

has order 42135.

Under this system it is possible to "move" the space to any square without changing the order of the arrangement. In addition, it is possible to change the order of the arrangement by transferring one number over any adjacent two. For instance, moving the "2" into the space in the above example makes the order 41325. In general, the three numbers involved in this transfer ("2", "1" and "3" in the above) will at most occupy two adjacent rows. If they occupy a single row either the row above or below may be used in the following (hence the transfer is possible even if the numbers are all in the top or the bottom row). Bring the space up into these two rows (without changing the order) and "join" the rows at their ends. We now "rotate" this system of two rows until the numbers which we want jumped are opposite each other at one end of the system. Now bring the blank space around to be opposite the number we wish to transfer and push it in. Finally, rotate the system so that the numbers unaffected by the transfer resume their previous positions. [Note that there can be no such other numbers in a puzzle which only has two columns and the technique fails. Instead one could operate on the columns. In the case of a 2 × 2 puzzle the order can be made to be either 123 or 132, which (we'll see) is all we need.]

This transfer is all we need to convert any arrangement into one of two final forms, in the following way. First move "1" into its top-left corner position. Then transfer "2" back two positions at a time until it is either next to "1" or with one intervening number. In the latter case the intervening number is transferred forward two places. With "2" positioned we turn to "3", etc. In this way, we can position all but the final two numbers, which will either be in correct or inverted order. After moving the space to its correct position in the solution arrangement, we have two possible final arrangements, differing by one interchange. One must be odd (relative to the solution), the other even, and it's the latter to which all even arrangements can be converted. For the arrangement , is odd while is the intermediate even arrangement.

2	5	3
4	☒	1

1	2	3
5	☒	4

1	2	3
4	☒	5

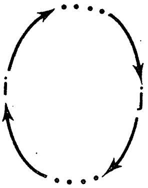
Of course, one should recognize that in solving a (possible) problem one would never actually make this conversion. Instead one would start with whatever was required in the top left corner of the solution and work through it in the snake-like order previously described.

The reader will now certainly appreciate how the explanation of the puzzle was made possible by characterizing a permutation with even-or-odd-ness, in such a way that interchanging any two numbers reversed the classification. To convince "non-mathematicians" of this property, Johnson illustrates it in a very neat way involving cycles. Consider the permutation, σ, written out as in the following example, for which $n = 6$.

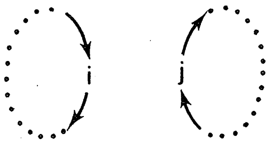
i	1	2	3	4	5	6
$\sigma(i)$	3	2	6	5	4	1

Start with a number, i, on the top row and write next to it the number, $\sigma(i)$, on the bottom row. Find this new number on the top row and write $\sigma(\sigma(i))$ the number underneath. Continue in this way until the initial number appears; forming a cycle. Thus beginning with $i = 1$ in the above we have 1361 as a cycle. Then choose a different number, i, and so on, thus separating into cycles - here 2 (on its own) and 45. Put m = (number of cycles found), here $m = 3$. Then $n - m$ will be odd or even (here $n - m = 6 - 3 = 3$, odd) and it turns out that this classification always agrees with the inverted pair method. They certainly agree for the case in which the numbers are in natural order - 1 2 3 ... n has n (single) cycles giving $n - m = 0$, even. All that remains to show is that any interchange of two numbers, i and j, will reverse the classification. There are only two cases to be considered (i) i and j are in the same cycle and (ii) in different cycles, represented in the diagrams below (where there may, or may not, be any numbers where the dots are shown).

(i)

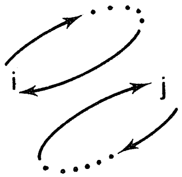


(ii)

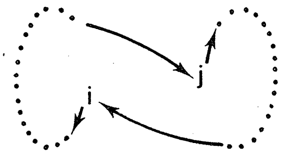


The effect of the interchange is to redirect, into j, any arrow going into i, and *vice-versa*. So after the interchange we have:

(i)



(ii)



One cycle is made into two, or two into one. Hence if $n - m$ is odd it will become even, if even, odd. Back to our puzzle, this cycle method provides a very quick way to determine parity of the (relative) permutation of an arrangement to a desired solution.

The even-or-odd-ness of the cycle property does not, however, seem directly related to that of the inverted-pair property. For there is no simple formula between the two (e.g. 2341 and 3214 both have three inverted pairs but, respectively one and three cycles, while 4313 has one cycle but 5 inverted pairs). Perhaps there are other properties reflecting this even-or-odd-ness of a permutation. The beauty of this system is, as rather grandly expressed by the editors of the 1879 Journal (in an attempt to explain why they would stoop to inserting articles on a puzzle):

> "...the principle of the game has its root in what all mathematicians of the present day are aware constitutes the most subtle and characteristic conception of modern algebra, viz: the law of dichotomy applicable to the separation of the terms of every complete system of permutations into two natural and indefeasible groups, *a law of the inner world of thought*, which may be said to prefigure the polar relation of left and right-handed screws, or of objects in space and their reflexions in a mirror."

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

I wish to propose for the reader's favourable consideration a doctrine which may, I fear, appear wildly paradoxical and subversive. The doctrine in question is this: that it is undesirable to believe a proposition when there is no ground whatever for supposing it true. I must of course, admit that if such an opinion became common it would completely transform our social life and our political system: since both are at present faultless, this must weigh against it.

Bertrand Russell, *On the Value of Scepticism,* 1935

* * *

For the rest, I do not deny that it is possible, by the consideration of limiting processes from a particular point of view, to prove rigorously the principles of the differential calculus, but the kind of metaphysics which it is necessary to use in doing so is, if not contrary, at least foreign to the spirit of analysis.

J.L. Lagrange, 1760.

LARGE PRIME NUMBERS

K.McR. Evans, Scotch College, Melbourne

(a) *Distribution of Primes*

A *prime* (number) is a natural number with exactly two distinct (natural number) factors. A natural number with more than two distinct factors is called *composite*. Thus the set of natural numbers, N, may be expressed as the union of the three disjoint sets: {primes}, {composites}, {1}. The first few primes may be listed as follows:

p_1	p_2	p_3	p_4	p_5 ...
2	3	5	7	11 ...

There does not appear to be a formula giving the nth prime, p_n, in terms of n. However as n increases it can be said that, "on average" the interval between successive primes increases. In fact, if you think of any large number, say 8000 000, it is possible to construct an interval with that number (8000 000) of consecutive numbers all of which are composite. The question immediately arises, "Is the number of primes finite?" The answer and its proof, known to Euclid (*circa* 300 B.C.), are given in theorem 1 which is then used in the construction of an interval of, say, 8000 000 consecutive composite numbers.

THEOREM 1: *The number of primes is infinite.*

Proof: Assume, instead, that the number of primes is finite. This is equivalent to assuming that there is a largest prime, say p_m, for some natural number m. Now consider the number

$$n = p_1p_2p_3\cdots p_m + 1.$$

n is larger than p_m. Also n is not exactly divisible by p_1 or by p_2 or ... or by p_m, there being a remainder of 1 in each case. Hence if n is composite, it must have prime factors larger than p_m. Otherwise n is prime. In both cases there is a prime larger than p_m and this contradicts the original assumption. Hence the assumption is false, and the number of primes is infinite.

To construct 8000 000 consecutive composite numbers first choose a prime p_m larger than 8000 000. This is possible since the number of primes is infinite. (p_m doesn't have to be known, though one such prime is 8004 119.) Next consider the numbers:

$$p_1 p_2 \cdots p_m + 2$$
$$p_1 p_2 \cdots p_m + 3$$
$$p_1 p_2 \cdots p_m + 4$$
$$\vdots$$
$$p_1 p_2 \cdots p_m + p_m$$

Each of these consecutive numbers is composite - explain why - and there are $p_m - 1$ numbers in the list. The construction thus gives at least 8000 000 consecutive composite numbers, and the result may be generalized to intervals of any length. On the other hand, N.G. Tchudakov, a Russian mathematician, has shown that, beyond some point, say for $n > N$, there is at least one prime between each successive pair of the numbers

$$1^4, 2^4, 3^4, \ldots, n^4, (n+1)^4, \ldots \ .$$

It may be true that the same statement is true for the sequence

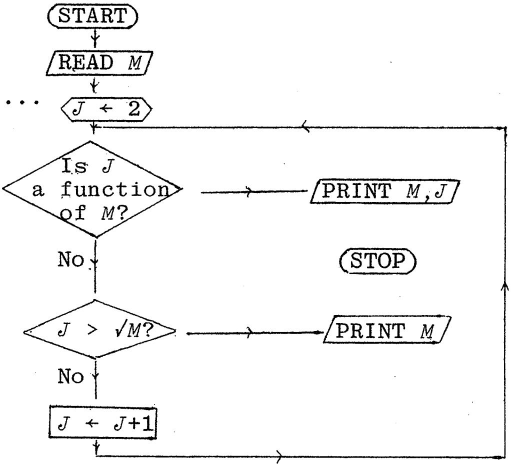
$$1^2, 2^2, 3^2, \ldots, n^2, (n+1)^2 \ldots,$$

but this has not been proved.

Incidentally, the next odd number after the prime 8000 119, *viz*. 8004 121, is also prime. Any two consecutive odd numbers, each of which is prime, are said to form a *prime pair*, e.g., (3,5),(5,7),(17,19),... . C. Goldbach, a Russian mathematician, 1690-1764, suggested that the number of such prime pairs is infinite. This conjecture has not yet been proved or disproved.

(b) *Testing for Primes*

The following flow chart shows an algorithm for testing whether or not a number, M, ($M > 2$) is prime. If M is prime, it is printed alone; if composite, it is printed with its smallest factor, J, (other than 1).



Set J equal to 2 ...

It is not necessary to test for factors larger than $\sqrt{M}$. Why?

Add 1 to J

The algorithm appears to be suitable for testing with a computer. Thus in BASIC, the factor test is performed by a statement such as

```
30 IF INT (N/J)*J = N THEN 40
```

and, in FORTRAN, by a statement such as

```
IF(N/J*J.EQ.N) GO TO 40.
```

However there are difficulties with very large numbers. For example if $M = 10^{100} + 1$, so $\sqrt{M} \simeq 10^{50}$ the time taken to perform the algorithm can be estimated as follows. Suppose a *fast* computer is able to perform each loop of the algorithm in 10^{-6} seconds. Since there are approximately 10^{50} loops to be executed, if M is prime, the possible time taken is approximately

$$\begin{aligned} & 10^{50} \times 10^{-6} \text{ seconds} \\ = {} & 10^{44} \text{ seconds} \\ \simeq {} & \frac{10^{44}}{3600 \times 24 \times 365} \text{ years} \\ > {} & \frac{10^{44}}{4000 \times 10\,000} \text{ years} \\ = {} & \frac{10^{44}}{4 \times 10^{7}} \text{ years} \\ > {} & 2 \times 10^{36} \text{ years.} \end{aligned}$$

Even if the algorithm is shortened by testing the values 2, 3 of J separately and then increasing J by 2 (so that only odd numbers are thereafter tested as factors of M) the time taken would still be greater than 10^{36} years. Thus it is not remotely feasible to use the algorithm on *any* computer for such large numbers.

(c) *Looking for Large Primes*

One way of generating large numbers, which may be prime, is to consider elements of

$$\{n : n = a^m \pm 1,\ a \in N \setminus \{1\},\ m \in N\} = S.$$

The following theorems, the proofs of which are left as exercises, mean that only certain proper subsets of S need be considered.

THEOREM 2: *If $a \geqslant 2$ and $a^m + 1$ is prime, then a is even and m is a power of 2.*

THEOREM 3: *If $m > 1$ and $a^m - 1$ is prime then $a = 2$ and m is prime.*

P. Fermat, a French mathematician, considered (in virtue of heorem 2) elements of the set of so-called Fermat numbers, *viz.*,

$$\{n : n = 2^{(2^m)} + 1 = F_m,\ m \in N \cup \{0\}\} = T.$$

e conjectured, *circa* 1650, that each element of T is prime. hus $F_0 = 2^{(2^0)} + 1 = 3$, $F_1 = 2^{(2^1)} + 1 = 5$, $F_2 = 2^{(2^2)} + 1 = 17$, $_3 = 2^8 + 1 = 257$, $F_4 = 2^{16} + 1 = 65\,537$ are all primes, but ut L. Euler (Swiss) showed in 1732 that $F_5 = 2^{32} + 1 =$ 41 × 6700 417, and is thus composite. There is a remarkable onnexion between Fermat numbers and geometry which was discovered by C.F. Gauss, a great German mathematician, at the age f eighteen. Gauss proved that, if n is prime and also a Fermat umber, then it is possible, using only straight-edge and ompasses, to construct a regular polygon of n sides, but if n is prime of any other form (e.g. 7, 11, 13) the construction is ot possible. The construction is also possible if n is the roduct of *different* Fermat primes (e.g. 3 × 5 but not 3 × 3) nd if $n = 4$; and finally if it is possible to construct a egular polygon of n sides, it is possible to construct one of n sides.

In 1958 R.M. Robinson at the University of California, erkeley, U.S.A., investigated elements of

$$\{n : n = k2^m + 1,\ m \in N,\ k \text{ is odd},\ 0 < k < 2^m\} = U$$

sing a theorem of F. Proth (1878).

Special case of Proth's theorem: If k is not a multiple of ; then $n = k.2^m + 1$ (an element of U) is prime if and only if n s a factor of $3^{(n-1)/2} + 1 = l$ (say).

To make this clearer two examples are considered.

(i) If $k = 1$, $m = 3$ then $n = 2^3 + 1 = 9$ and $l = 3^{(9-1)/2} + 1 = 82$. Since n is not a factor of l, by Proth's theorem it is not prime (as we know).

ii) If $k = 7$, $m = 4$, then $n = 7 \times 2^4 + 1 = 113$ and $l = 3^{(113-1)/2} + 1 = 3^{56} + 1$. The test to see whether or not n is a factor of l is suitable for a computer since only one division (though a complex one) is required.

Using a computer, Robinson verified that the Fermat number $_n$ is *not* prime if $5 \leqslant n < 12$. In fact, no larger Fermat prime han F_4 is known. The largest prime Robinson discovered using roth's theorem is $n = 5 \times 2^{1947} + 1$. To estimate the number of igits in n, the following method may be employed:

$$\begin{aligned} n &= 5 \times 2^{1947} + 1 \\ &> 2^2 \times 2^{1947} \qquad (\text{since } 5 > 2^2) \\ &= 2^{1949} \\ &= (2^{10})^{194 \cdot 9} \\ &> (10^3)^{194 \cdot 9} \qquad (\text{since } 2^{10} = 1024) \\ &= 10^{584 \cdot 7} \\ &> 10^{584}. \end{aligned}$$

10^{584} has 585 digits whereas actually n has 587 digits.

The largest currently known prime has the form suggested by theorem 3. It is

$$2^{19937} - 1$$

which has 6002 decimal digits, and was shown to be prime in just under 40 minutes on a computer by B. Tuckerman of New York in 1971.

(d) *An Application*

Large primes were investigated without any thought of practical use. Recently, however, they have been used in coding messages in an apparently unbreakable cypher. The method was developed by R. Rivest at the Massachusetts Institute of Technology.

A message is converted by any suitable conventional coding method into a number, M. M is raised to the power S: S being chosen as, say, 10^4 so that M^S is very large. M^S is divided by a number N which is the product of two large primes P,Q (each greater than 10^{40}). The remainder, C, after division is the finally coded message which is transmitted. C, and even N, can be made public, but not P and Q. Finding large factors of a number cannot be done by a computer as we have seen in (b). When the message, C, is received it is decoded (as M) by raising C to a certain power T, and finding the remainder when C^T is divided by N. T can only be calculated if P and Q are both known.

References

Enrichment Mathematics for High School; National Council of Teachers of Mathematics, Washington D.C., U.S.A., 1963.

An Introduction to the Theory of Numbers (3rd edition); G.H. Hardy and E.M. Wright; Oxford University Press, U.K., 1954.

Men of Mathematics, Vol.1; E.T. Bell; Penguin Books, U.K.,1953.

New Scientist, Vol.77, No.1092, 2nd March 1978, p.594.

Guinness Book of Records, 23rd Edition (Australian), October 1976, p.81.

* * * * * * * * *

CALCULUS BY ACCIDENT?
G.A. Watterson, Monash University

Finding the area of a plane region is easy if the region has a boundary with straight edges, for instance when it is a triangle, a rectangle, or a more complicated polygon. But when part of its boundary is curved, the area is not so easy to find. Of course, every one knows that the area of a circle of radius r is πr^2, but the number π is not a simple quantity as it is evaluated only by some limiting process. Again, the areas of elliptical regions, and various other such areas, are given by simple-looking formulas but usually they are derived by advanced methods, particularly by integration.

In this article, certain random experiments are conducted to estimate areas, and to evaluate integrals.

Suppose that we wish to find the area of the shaded region in Figure 1, that is, the area under the function $g : [0,1] \to [0,1]$, between $x = 0$ and $x = 1$.

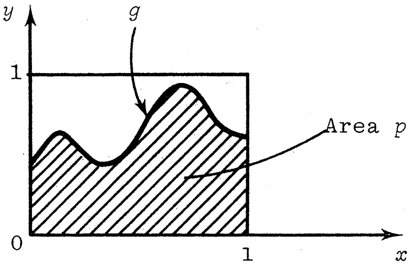


Figure 1

We are assuming that the function g takes values between 0 and 1 over its domain:

$$0 \leqslant g(x) \leqslant 1 \text{ for all } x \in [0,1].$$

If our problem were not of this precise form originally, we might be able to change it to the above form by changing the scales on our axes, by rotating and translating our region if necessary, etc.

The required shaded area is

$$p = \int_0^1 g(x)dx,$$

while the area of the square region

$$\{(x,y): 0 \leqslant x \leqslant 1, 0 \leqslant y \leqslant 1\},$$

is 1. Thus our required area is the *proportion* of the unit area which is shaded.

METHOD 1.

Now, a standard method for estimating what proportion of Melbourne's population watches T.V. is to choose a random sample of people (the more people the better) and ask them. We estimate the proportion of Melbourne people who watch T.V. by the proportion who do so in our sample. Similarly, to estimate the proportion of the square region which is shaded in Figure 1, we might choose a number of points at random from that square, and calculate the proportion of these points which fall in the shaded region.

EXAMPLE

As an example, consider the problem of estimating the area under $g(x) = \sin x$ between $x = 0$ and $x = 1$, that is, of finding

$$\int_0^1 \sin x \; dx.$$

I found the following ten random numbers printed in the Hewlett-Packard HP 25 calculator program book: 0·14, 0·76, 0·15, 0·35, 0·62, 0·54, 0·62, 0·91, 0·48, 0·24. The same book gives a program for calculating further random numbers (i.e. numbers uniformly distributed between 0 and 1) if you need them. But these ten numbers will do for our example. Let us pair the numbers off to represent the (x,y) co-ordinates of five points from the unit square:

$$P_1 = (0{\cdot}14,0{\cdot}76),\ P_2 = (0{\cdot}15,0{\cdot}35),\ P_3 = (0{\cdot}62,0{\cdot}54),$$
$$P_4 = (0{\cdot}62,0{\cdot}91),\ P_5 = (0{\cdot}48,0{\cdot}24).$$

These points are plotted in Figure 2, together with the sin x curve.

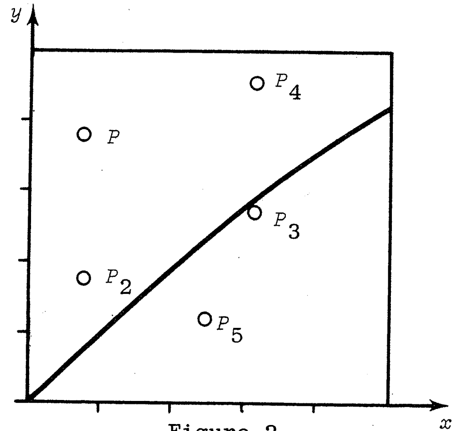


Figure 2

We see that two points, P_3 and P_5, out of the five fall inside the shaded area, so we could say

$$\int_0^1 \sin x \, dx \simeq 2/5 = 0{\cdot}4.$$

Of course, the correct value is

$$\int_0^1 \sin x \, dx = \cos 0 - \cos 1 = 0{\cdot}4597.$$

In this example we happen to know the correct answer from tables (someone has already calculated cos 1 for us) and it turns out to be quite close to our estimated value.

METHOD 2

The above method of estimating the area is not the *best* method, even among those methods employing random experiments. A better use of the random numbers is the following.

Suppose that $g(x)$ is defined for $0 \leqslant x \leqslant 1$ and that we wish to estimate the value of the integral

$$\int_0^1 g(x)dx.$$

If we take n random numbers, $x_1, x_2, \ldots, x_n$, and calculate $g(x_1), g(x_2), \ldots, g(x_n)$, then the average of these should be close to the average height of the function $g(x)$. Hence we have

$$\frac{g(x_1) + g(x_2) + \ldots + g(x_n)}{n} \simeq \int_0^1 g(x)dx.$$

EXAMPLE

To estimate $\int_0^1 \sin x \, dx$, we might take the ten random numbers used in the previous method and calculate the average of their sines. We have:

x	0·14	0·76	0·15	0·35	0·62	0·54	0·62	0·91
sin x	0·1395	0·6889	0·1494	0·3429	0·5810	0·5141	0·5810	0·7895

x	0·48	0·24
sin x	0·4618	0·2377

and the average of the ten sin x values is 0·4486. This is really quite close to the integral's value 0·4597, and could be made much closer if more than ten random numbers were used. I tried 100 random numbers, and found the estimate as 0·4568 which has less than 1% error.

METHOD 3

A further improvement in accuracy can be achieved by using each random number *twice*. We use the random number once in the form x, and again as $1 - x$. The estimation is done according to

$$\frac{g(x_1)+g(1-x_1)+g(x_2)+g(1-x_2)+\ldots+g(x_n)+g(1-x_n)}{2n} \simeq \int_0^1 g(x)dx.$$

EXAMPLE

Using Method 3 and the random numbers of the previous examples, we now augment the ten sin x values used before with the corresponding ten sin$(1 - x)$ values. You may check that the average of all twenty values is 0·4650. Using 100 random numbers I found the average of 200 sin x and sin$(1 - x)$ values as 0·4593, which has less than 0·1% error. To use these random experiments for estimating areas, a good supply of random numbers is required. Any number of computer programs are available to generate them, and there are table books devoted to them. "Random numbers are too important to be left to chance."

Accuracies of the methods.

To be honest, although we shall now show that Method 2, which is generally better than Method 1, yet for simple examples such as ours, non-random methods may be better still. For instance, Simpson's Rule (see *Function* 1977, Vol.1, part 1, page 17 and part 5, page 25) using 10 intervals is better than Method 3 with 100 random numbers! There are two things to be said in favour of the random experiments (called "Monte Carlo" methods after the Casino at Monte Carlo). They can be used with virtually no more difficulty to estimate volumes, and the content of higher dimensional regions, whereas deterministic methods require greater sophistication. The random methods also allow us to use statistical theory to describe their accuracy, whereas the accuracy of deterministic methods is harder to evaluate.

Consider Method 1. The number of random points, out of n, which fall into the shaded region in Figure 1 has a binomial probability distribution. The mean number is np, where $p = \int_0^1 g(x)dx$, and the variance is $np(1 - p)$. The *proportion* of points falling in the shaded region has mean p and variance

$$\sigma_1^2 = p(1 - p)/n.$$

Knowing that the proportion is very likely to be within two standard deviations from its mean, we can say that the estimate should be within $\pm 2\sigma_1 = \pm 2\sqrt{p(1 - p)/n}$ of its mean. For instance, with $p = 0{\cdot}4597$ as in our example, and using $n = 5$ points, the estimate 0·4, should be within a distance $2\sigma_1 = 0{\cdot}4458$ from p. Of course it is much closer than that, in fact. Using $n = 1000$ points would similarly very likely get us within 0·0315 of p.

The second method uses the average of n values of the random variable $Y = g(X)$. Each one has variance

$$\text{Variance } Y = E(Y^2)-(E(Y))^2 = \int_0^1 (g(x))^2 f(x)dx - \left[\int g(x)f(x)dx\right]^2$$
$$= \int_0^1 (g(x))^2 dx - p^2.$$

But as $0 \leqslant g(x) \leqslant 1$, then $(g(x))^2 \leqslant g(x)$, and so

$$\int_0^1 (g(x))^2 dx \leqslant \int_0^1 g(x)dx = p.$$

Thus

$$\text{Variance } Y \leqslant p - p^2 = p(1 - p),$$

and, if $\overline{Y}$ is the average of n independent Y's, we get

$$\text{Variance } \overline{Y} = \sigma_2^2 = (\text{Variance } Y)/n$$
$$\leqslant p(1 - p)/n = \sigma_1^2.$$

Because $\sigma_2^2 \leqslant \sigma_1^2$, the second method is at least as accurate as the first. In fact, a fairer comparison would be between Variance $Y/(2n)$ and σ_1^2, because, if the first method uses n points it also involves $2n$ random numbers, and the second method could be based on $2n$, rather than n, random numbers to be comparable. For instance, $n = 5$ points in Method 1, with $2\sigma_1 = 0{\cdot}4458$, corresponds to 10 random numbers, for which $2\sigma_2 \leqslant 2\sqrt{p(1-p)/10} = 0{\cdot}3152$ in our example.

The third method is more accurate still, as it uses each random number twice. Admittedly X and $1 - X$ are not *independent* random numbers, so we haven't really doubled our random numbers and halved our variance, but the effect is in that direction.

Problem: Calculate $\int_0^1 x^2(1 - x)^3 dx$ by calculus methods, and by some of the above methods.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

SOLUTION TO PROBLEM 3.3 (from Ravi Sidhu, age 13, Ignatius Park College, Townsville).

The problem is to find a winning strategy for the following game.

Blackjack or Twenty-one. Two players in turn take from a pile of 21 matches. At each turn a player must take at most 5 matches and at least 1 match. The player who takes the last match wins.

If you start first, always take away 3 matches, leaving your opponent with 18 matches. On your next turn take away an amount of matches that will leave your opponent with 12 matches. (Your opponent couldn't have left you with 12 matches because the maximum he can take from 18 matches is 5, leaving 13 matches.) On your next turn take away an amount of matches that will leave your opponent with 6 matches. When your opponent is faced with 6 matches, the maximum he can take away is 5 matches, and you take away the last match, winning the game. If you start first and always take away 3 matches, there is no way that your opponent can win.

* * *

RAVI SIDHU also gave a program for Problem 1.4 which instead of checking all numbers from 1 to 1000 for the required properties selected ten numbers at random and printed the full sequence for each.

He also asked for articles on computer programming.

* * *

PROBLEM 4.1

Simplify the following statement:

If Monday is a public holiday, then I will not go to the beach, or I will stay at home, or I will neither stay at home nor go to the beach.

PROBLEM 4.2

There are 700 hymns in a church hymn book. It is required to print a set of cards, each with one digit on it, so that the numbers of any four hymns (to be sung on Sunday) can be displayed on a notice board. How many cards are required? (Give two answers, one assuming that an inverted 6 can be used as a 9, the other without that option.)

PROBLEM 4.3

Find the number of 0's at the end of the number 1000! (See *The Accursed Calculator*, p.5 of this issue.)

PROBLEM 4.4

From the roof of a 300 metre building in New York, two marbles are dropped, one being released when the other has already fallen 1 mm. How far apart will they be when the first hits the ground?

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

THERE IS NO RECIPE AND WHAT IT IS

I think I can tell someone how to write, but I can't think who would want to listen. The ability to communicate effectively, the power to be intelligible, is congenital, I believe, or, in any event, it is so early acquired that by the time someone reads my wisdom on the subject he is likely to be invariant under it. To understand a syllogism is not something you can learn; you are either born with the ability or you are not. In the same way, effective exposition is not a teachable art; some can do it and some cannot. There is no usable recipe for good writing.

Then why go on? A small reason is the hope that what I said isn't quite right; and, anyway, I'd like a chance to try to do what perhaps cannot be done. A more practical reason is that in the other arts that require innate talent, even the gifted ones who are born with it are not usually born with full knowledge of all the tricks of the trade. A few essays such as this may serve to "remind" (in the sense of Plato) the ones who want to be and are destined to be the expositors of the future of the techniques found useful by the expositors of the past.

The basic problem in writing mathematics is the same as in writing biology, writing a novel, or writing directions for assembling a harpsichord: the problem is to communicate an idea. To do so, and to do it clearly, you must have something to say, and you must have someone to say it to, you must organize what you want to say, and you must arrange it in the order you want it said in, you must write it, rewrite it, and re-rewrite it several times, and you must be willing to think hard about and work hard on mechanical details such as diction, notation, and punctuation. That's all there is to it.

P.R. Halmos, *How to Write Mathematics*, 1973.

∞ ∞ ∞ ∞ ∞

Look around when you have got your first mushroom or made your first discovery; they grow in clusters.

G. Polya, *How to Solve it*, 1945.

∞ ∞ ∞ ∞ ∞

"Take some more tea," the March Hare said to Alice, very earnestly.

"I've had nothing yet," Alice replied in an offended tone: "so I can't take more."

"You mean you ca'n't take *less*," said the Hatter: "it's very easy to take *more* than nothing."

Lewis Carroll, *Alice's Adventures in Wonderland*.