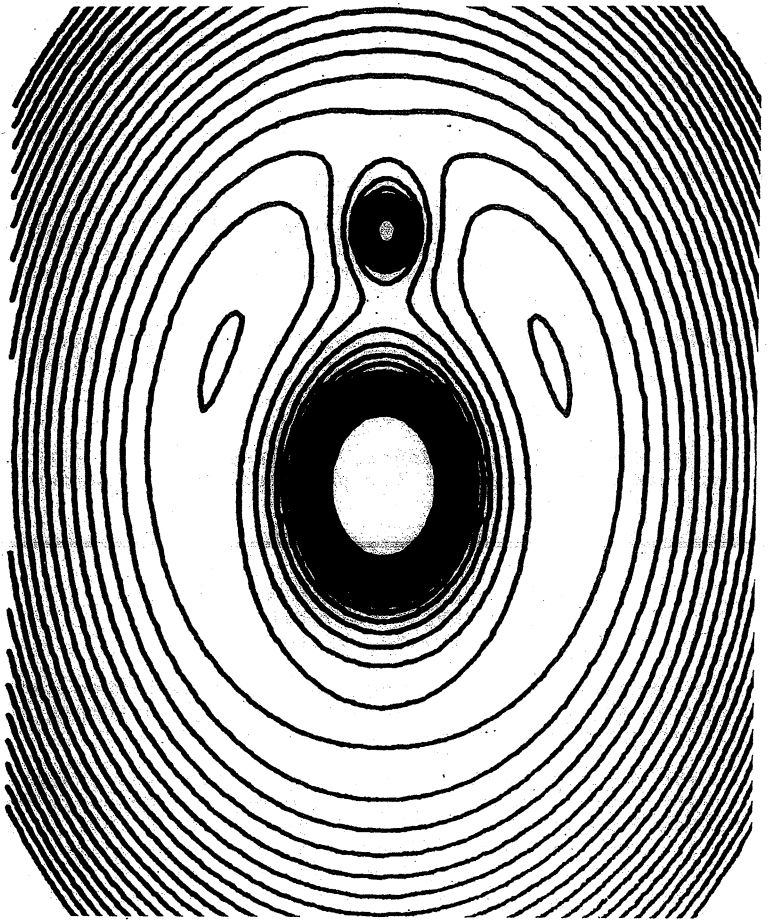
ISSN 0313 - 6825

FUNCTION

Volume 8. Part 5 October 1984



A SCHOOL MATHEMATICS MAGAZINE

Published by Monash University

Reg. by Aust. Post Publ. No. VBH0171

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 mathematics departments of the institutions shown above.

The magazine is published five times a year, appearing in February, April, June, August, October. Price for five issues (including postage): $8.00*; single issues $1.80. 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.

*$4.00 for *bona fide* secondary or tertiary students.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

Registered for posting as a periodical - "Category B"

For those studying probability theory, this issue of *Function* will be of special interest. Dr Tim Brown, formerly of Monash University and now working at the University of Melbourne, has described some aspects of his recent research on the Poisson distribution. This is one of the basic distributions studied in school syllabuses, but it has aspects that go well beyond this. Dr Brown's recent work appears in full in *American Mathematical Monthly* (Feb. 1984) and one aspect of it is summarised here.

CONTENTS

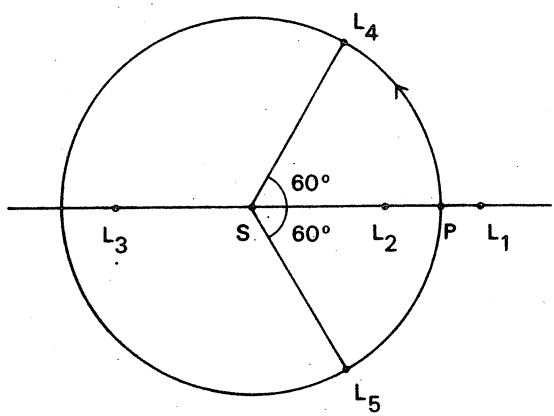
THE FRONT COVER

Suppose a planet circles round a sun and further suppose that a small body is introduced into the combined gravitational field of these two bodies. This third body is subject to three forces:

(a) the gravitational attraction of the sun,
(b) the gravitational attraction of the planet,
(c) the centrifugal force caused by the rotation of the system.

(It would be possible to recast the working in terms of a fixed set of axes and so avoid this last force, but this makes the calculation much more complicated.)

There are five points at which the third body may remain at rest (relative to the sun and its planet). These are indicated in the diagram below as L_1, L_2, L_3, L_4, L_5. They are the so-called Lagrangian points (named after the mathematician and astronomer J.L. Lagrange, 1736-1813, who discovered them).



At L_1, the combined gravitational pull of sun, S, and planet, P, to the left exactly counteracts the centrifugal force acting to the right. A similar analysis applies to L_3 (with left and right interchanged).

At L_2, the (stronger) leftward attraction of S is balanced by the sum of the (weaker) rightward pull of P and the centrifugal force.

Two other Lagrangian points, L_4, L_5, also exist. These lie 60° ahead of and behind the planet in its orbit around the sun. Analysis of these equilibria requires vector diagrams and is left to you to complete.

Equilibria are classified as being either *stable* or *unstable*. A pivoted rod hanging with its centre of mass below its point of support is in stable equilibrium. Such a rod with its centre of mass poised above the point of support is in equilibrium but is unstable and will eventually fall.

A particle situated at L_1, L_2 or L_3 is in unstable equilibrium, and so we do not expect these points to be as significant astronomically as L_4, L_5. The point L_2 has a theoretical significance for moon-probes which (as some accounts rather loosely put it) pass through or near this "point of zero gravity".

Some authors believe that there is a cloud of small particles to be found at the point L_1 in the sun-earth system and that these are sometimes seen as the *gegenschein* (or counterglow), a faint brightness in the night sky 180° from the position of the sun. Calculations have shown that although in this case L_1 is unstable, particles tend to linger near it for a long time if they arrive there. Other authors dispute this explanation, doubting that meteoric particles would reach L_1 in sufficient numbers.

L_4, L_5 are points of stable equilibrium. In the sun-Jupiter system they are occupied by the so-called Trojan asteroids. The corresponding points of the earth-moon system are also occupied by what might be thought of as two further natural satellites of the earth, but as these are extremely faint dust clouds they usually pass unremarked.

Our cover diagram comes from a computer simulation of such systems and was produced by Professor R.F.E. Van der Borght of Monash University. L_4, L_5, the stable points, appear as oval regions and are readily visible. L_1, L_2, L_3 are less obvious. L_2 may be seen as an X-shaped patch between the sun and the planet, and, in principle, such patches could be made to appear near L_1 and L_3. This, however, would have cluttered up the picture too much, so, in the interests of clarity, they were omitted.

You may like to explore some of this for yourself. Remember that a planet and sun revolve around their common centre of mass (assume the mass of the small body is too tiny to disturb this appreciably) and that the centrifugal force on the planet as it circles around this exactly balances its gravitational attraction toward the sun. For a body at L_4, say, two components of force must cancel. The centrifugal force out from the centre of mass exactly equals the attraction toward that point and motion at right angles to this direction is prohibited by the exact balance of attraction toward the sun and attraction toward the planet.

TURING MACHINES[†]

J.N. Crossley, Monash University

Alan Turing was a British mathematician whose work on computers underlies much of their present-day theory. Although he worked on the actual construction of computers, as well as on their theoretical description, he is best remembered for his work on computability, which he was the first to characterise in a full and rigorous way.

To do this he devised what are today called *Turing machines*, rather simple machines but extremely versatile ones. It is now almost universally agreed that if a function is computable at all, then it is computable by such a machine. Note, however, that when one speaks of a "machine" in this context, one is not just talking of an actual machine such as an Apple or a Commodore, but of any conceivable *abstract* machine.

Such a machine is defined mathematically and, although you could build a Turing machine (and some of my students have simulated them on the Monash computers), Turing machines are more important from the point of view of ideas rather than of practicalities.

Turing machines appear very simple and in many ways they *are* simple. They can, however, treat very complicated problems indeed. In particular, as remarked earlier, *all* functions computable by *any* computer, no matter how powerful, can be computed by Turing machines.

What is a Turing Machine?

A Turing machine consists of two parts:

1. A reading-and-writing head.
2. A tape.

The tape, which can be indefinitely extended to both left and right, is marked out in squares on which symbols can be written by the head. The set of possible symbols (e.g. those available on a keyboard) is called the *alphabet* and is finite. The symbols are usually denoted by $S_0, S_1, \ldots, S_m$.

[†]The original version of this paper was given as the first lecture in the University of the Philippines Diamond Jubilee mathematics lectures in November 1982 and will appear in the journal *Matimyás Matematika*.

The machine itself is considered to have a finite number of *internal states* or machine configurations (analogous to the various states in which an electronic computer finds itself). These are usually denoted by $q_0, q_1, \ldots, q_n$.

A Turing machine is characterised by its *program*, which consists of a set of instructions of the form

$$q\ S\ L\ q'$$

which is interpreted as:

> *If in state* q, *reading symbol* S *on the tape, move one square to the left and go into state* q'.

The instruction

$$q\ S\ R\ q'$$

is interepreted in the same way, but the word "left" is replaced by "right".

The instruction

$$q\ S\ S'\ q'$$

is interpreted as:

> *If in state* q, *reading symbol* S *on the tape, replace this by symbol* S' *and go into state* q'.

Numbers may be represented on the tape by using S to represent the number 0, SS the number 1, SSS the number 2 and so on. (We use S to represent the number 0 to distinguish the number 0 from a blank tape.)

The concept of program distinguishes versatile computers from the earlier hard-wired models. Before the work of John von Neumann in the mid 1940's, computers had fixed configurations and could only compute specific functions (rather like the non-programmable pocket calculators of today). Von Neumann invented programmable machines and the theoretical idea behind these is that of a universal Turing machine.

Programs for Turing machines consist of finite sets of instructions, each involving finitely many elements $S_0, S_1, \ldots, S_m$; $q_0, q_1, \ldots, q_n$; L, R). To each element on this list we assign a number as follows:

$$q_0 \to 3,\ S_0 \to 5,\ q_1 \to 7,\ S_1 \to 9,\ \ldots,\ L \to 2,\ R \to 4.$$

Then we can code (e.g.) $q_0\ S_1\ L\ q_1$ in the following manner. First write down the corresponding numbers (3 9 2 7). Next use these as exponents of the first few prime numbers (2,3,5,7,...) and multiply. This gives

$$2^3.3^9.5^2.7^7,$$

a very large number, but this is not a problem. We note that *every* number may be decomposed into primes in one and only one way. (This is called the unique factorisation theorem or the fundamental theorem of arithmetic.)

So if

$$n = 2^{n_0}.3^{n_1}.5^{n_2}.7^{n_3}.11^{n_4} \ldots$$

we can recover the numbers $n_0, n_1, \ldots$ from the single number n. These exponents can then be decoded to give the original string of elements - in our case the exponents are 3, 9, 2, 7 corresponding to $q_0 S_1 L q_1$.

By using more and more primes we can code longer expressions. In particular we can code those programs of Turing machines. Any particular Turing machine is characterised by its program. This machine may then also be represented by the number m which codes its program along the lines described above.

The Universal Machine

Suppose now a machine represented by the number m acts on an input represented by the number x. We may now construct a machine U which will act in exactly the same way as the first machine if U has on *its* tape the representation of the number pair (m,x). U does this by digging out the mth set of instructions from the coding and then applying these to simulate a tape with x represented on it.

So now we have one Turing machine which will compute all computable functions of the one argument x and it is easy to generalise to other numbers of arguments. (Merely replace x in the above reasoning by $x_1, x_2, \ldots, x_n$.)

There is an apparent paradox here however. The machine U will compute all functions that can be computed. This is not to say however that it can compute all functions. It cannot. There are uncountably many functions, but the universal machine can compute only countably many - one for each Turing machine encoded. (See the articles on Infinite Numbers in *Function Vol.2, Parts* 1,2.)

It follows that there exist non-computable functions and these represent unsolvable problems in the sense that there is no mechanical procedure for solving them. Examples of such problems abound and it is easy to give one. This we now proceed to do.

The Halting Problem

This is the so-called *Halting problem*. We ask whether there is a machine which will tell us whether Turing machine number m will halt (i.e. come to a stop rather than go into a loop or otherwise calculate endlessly) when presented with the input x.

Suppose such a machine does exist. Call it H. Now construct a new machine G which depends on H as follows. Let $U(m,x)$ be the value computed by the universal machine for the input (m,x).

Then set

$$G(x) = \begin{cases} U(x,x) + 1 & \text{if machine } x \text{ halts on input } x \\ 0 & \text{if not.} \end{cases}$$

This function is clearly computable assuming H exists. Now, however, let g be the number of the machine G. We consider $G(g)$. G must eventually halt because $G(x)$ has a value for every x, in particular for g. Thus, if we put $x = g$ in the formula above, we find that

$$G(g) = U(g,g) + 1 .$$

But $U(g,x)$ is the value computed by the universal machine for input (g,x) and this is the same as the value computed by the machine G for input x that is to say $G(x)$. Now put $x = g$ and we find

$$G(g) = U(g,g) .$$

But by the definition of G given above

$$G(g) = G(g) + 1 ,$$

which is a contradiction.

It follows that our assumption that H exists is false. We thus have the

THEOREM: The halting problem for Turing machines is not computable.

Computability.

Turing machines have proved immensely valuable and have given us great insight into the concept of computability. The notion of computability however does not depend on the rather special character of Turing machines. There are several other definitions of computability. What is really surprising is that all the formal, mathematical definitions give *exactly* the same computable functions. Mathematicians generally agree that our intuitive idea of 'computable' really means the same as 'computable on a Turing machine': no more and no less.

Perhaps most surprising of all is the fact that Turing invented the mathematical notion of Turing machines *before* he started building computing machines at the National Physical Laboratory in London and yet all the things that can be computed on any modern computer can already be computed by his abstract Turing machines.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

For an example of a calculation involving a Turing machine, see p.13. (*Eds*)

EUCLID'S ALGORITHM†

J.A. Deakin,
Shepparton College of TAFE

In your early mathematical training you almost certainly learnt to find the highest common factor (HCF) and lowest common multiple (LCM) of two positive integers a and b by first expressing a and b as a product of prime factors. Thus for the numbers 540 and 168 we have

$$540 = 2^2 \times 3^3 \times 5$$

$$168 = 2^3 \times 3 \times 7.$$

The highest common factor is $h = 2^2 \times 3 = 12$. The lowest common multiple is $m = 2^3 \times 3^3 \times 5 \times 7 = 7560$.

However, this procedure is only satisfactory when the resolution into prime factors can be carried out easily by inspection. If the numbers a and b are large, it is inconvenient to spend time seeking prime factors, and a much more efficient procedure is to use Euclid's algorithm.

We say that an integer b ($\neq 0$) is a divisor of an integer a if and only if there is an integer q such that $a = qb$. More generally, if a and b are any positive integers, there exist non-negative integers q and r such that

$$a = qb + r, \quad 0 \leqslant r < b.$$

The integer q is called the quotient, and r the remainder when a is divided by b.

The highest common factor (HCF) or greatest common divisor (GCD) of two integers a and b is the unique positive integer h which has the two properties:

(i) h divides both a and b,
(ii) if c is any positive integer which divides both a and b, then c divides h.

In order to determine h, we use the following process:

---

†Many of the ideas in this article relate closely to those used in modular arithmetic as discussed by Perdix in his recent columns.

Assume that $b < a$, and divide a by b to give the quotient q_1 and remainder r_1.

Divide b by r_1 to give the quotient q_2 and remainder r_2.

Divide r_1 by r_2 to give the quotient q_3 and remainder r_3, and so on.

Since $b > r_1 > r_2 > r_3 \ldots$, the sequence must end after a finite number of divisions, the last giving a zero remainder. At this point we stop. Suppose that $r_{n+1} = 0$. Then we may write the process as follows:

$$a = q_1 b + r_1, \quad 0 < r_1 < b \tag{1}$$

$$b = q_2 r_1 + r_2, \quad 0 < r_2 < r_1 \tag{2}$$

$$r_1 = q_3 r_2 + r_3, \quad 0 < r_3 < r_2 \tag{3}$$

$$\ldots$$

$$r_{n-2} = q_n r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \tag{4}$$

$$r_{n-1} = q_{n+1} r_n + 0. \tag{5}$$

We show that the HCF of a and b is the last non-zero remainder r_n in the Euclidean algorithm. To show that r_n divides both a and b, note that:

from (5), r_n divides r_{n-1},

hence from (4), r_n divides r_{n-2}.

Continuing in this way, from (2) we find that since r_n divides r_1 and r_2, it also divides b, and from (1) it divides a. Also, if c is any integer which divides a and b,

from (1), c divides r_1

from (2), c divides r_2

from (4), c divides r_n.

Hence the HCF of a and b is the last non-zero remainder r_n in the Euclidean algorithm.

Furthermore, we can show that if h is the HCF of a and b, then there exist integers (positive or negative) A and B such that

$$aA + bB = h.$$

Consider the set S of all integers of the form $aA + bB$. From (1), $r_1 \in S$. Substituting the expression for r_1 in (1) into (2), we see that $r_2 \in S$. Then continuing in this way, we see that every remainder is an element of the set S, and finally that r_n, the HCF of a and b is an element of S.

We illustrate the algorithm by means of the example used to introduce this paper,

$$540 = 3 \times 168 + 36 \quad (1)$$
$$168 = 4 \times 36 + 24 \quad (2)$$
$$36 = 1 \times 24 + 12 \quad (3)$$
$$24 = 2 \times 12 + 0 \quad (4)$$

Hence the HCF h of 540 and 168 is 12.

Also,

$$\begin{aligned} 12 &= 1 \times 36 - 1 \times 24 \quad \text{by (3)} \\ &= 5 \times 36 - 1 \times 168 \quad \text{by (2)} \\ &= 5 \times 540 - 16 \times 168 \quad \text{by (1).} \end{aligned}$$

We say that two positive integers a and b are relatively prime if and only if there exist integers A and B such that $aA + bB = 1$, i.e. when the HCF of a and b is 1. In particular, we note that if a and b are positive integers with HCF h, the integers a/h and b/h are relatively prime. The lowest common multiple (LCM) of two positive integers a and b is the unique positive integer m such that:

(i) a divides m and b divides m,
(ii) if c is any positive integer such that both a and b divide c, then m divides c.

We show that $m = ab/h$. For $a = 540$ and $b = 168$, $m = 540 \times 168 \div 12 = 7560$ as before. Let $a_1 = a/h$ and $b_1 = b/h$. Then $ab/h = a_1 b_1 h = ab_1 = ba_1$, i.e. both a and b divide ab/h. If a divides c, let $c = ra = ra_1 h$. If b divides c, let $c = sb = sb_1 h$. Then $ra_1 h = sb_1 h$, i.e. $ra_1 = sb_1$. Since a_1 and b_1 are relatively prime, a_1 divides s. Let $s = qa_1$. Then $c = qa_1 b_1 h = q(ab/h))$, so that ab/h divides c, which proves the theorem.

There are a number of interesting applications of Euclid's algorithm. Although it is easy to express the sum of two numerical fractions such as $2/5 + 3/7$ as a fraction with a single denominator,

$$2/5 + 3/7 = (14 + 15)/35 = 29/35$$

the reverse process of expressing a fraction such as 43/77 as a sum of fractions whose denominators are the factors of 77, i.e. in the form $a/7 + b/11$ is more difficult. Apart from methods of trial and error, the only procedure for doing so depends on Euclid's algorithm.

Since $11 = 1 \times 7 + 4$

$7 = 1 \times 4 + 3$

$4 = 1 \times 3 + 1$

$3 = 3 \times 1 + 0,$

we have $1 = 4 - 1 \times 3$

$= 2 \times 4 - 1 \times 7$

$= 2 \times 11 - 3 \times 7.$

Then $1/77 = (2 \times 11 - 3 \times 7)/77$

$= 2/7 - 3/11.$

Hence $43/77 = 86/7 - 129/11$

$= (12 + 2/7) - (12 - 3/11)$

$= 2/7 + 3/11.$

More generally, suppose that it is required to resolve $k/(ab)$ into such "partial fractions", where a and b are relatively prime. Since a and b are relatively prime, there exist integers A and B such that $aA + bB = 1$. Hence $(aA + bB)/ab = 1/(ab)$ and $k/(ab) = (kaA + kbB)/(ab) = kA/b + kB/a$ which gives the required partial fractions.

We can also apply Euclid's algorithm to find the solution of linear diophantine equations in two unknowns, i.e. we seek integers x,y which satisfy the equation

$$ax + by = c$$

where a,b,c are integers.

This equation has an unlimited number of solutions corresponding to the coordinates of the points on the straight line $ax + by = c$. If a and b have a factor k which does not divide c, the equation cannot be satisfied by integral values of x and y, since $ax + by$ is then divisible by k, and c is not. Hence we suppose that a,b,c have no common factor, and that a and b are relatively prime.

Since a and b are relatively prime, there exist integers x_1 y_1 such that

$$ax_1 + by_1 = 1$$
$$\therefore acx_1 + bcy_1 = c$$

and $x = h = cx_1$, $y = k = cy_1$ is clearly a solution of the original equation.

Then $ax + by = ah + bk$

$a(x - h) + b(y - k) = 0$

$\therefore (x - h)/b = (k - y)/a = t$, an integer

i.e. $x = h + bt$, $y = k - at$, which is the general solution. To

illustrate by means of an example, suppose that it is required to find all integers x,y which satisfy the equation

$$3x + 5y = 11.$$

From Euclid's algorithm, we find that

$$1 = 2 \times 3 - 1 \times 5$$
$$\therefore 11 = 22 \times 3 - 11 \times 5,$$

so that one solution of the equation is $x = 22$, $y = -11$. Then $3(x - 22) + 5(y + 11) = 0$ and $5(y + 11) = 3(22 - x)$ so that $(22 - x)/5 = (y + 11)/3 = t$, an integer, whence $x = 22 - 5t$, $y = 3t - 11$ $(t \in J)$ is the general solution.

The algorithm may also be used to solve linear congruences. If a and b are any two integers which when divided by m leave the same remainder, we say that a and b are congruent, modulo m. Then $a - b$ is a multiple of m, and we write

$$a \equiv b \pmod{m}$$

or

$$a - b \equiv 0 \pmod{m}.$$

If c is relatively prime to m, then the congruence $cx \equiv b \pmod{m}$ has an integral solution x. By hypothesis, the HCF of c and m is 1.

$$\therefore 1 = sc + tm \quad \text{for suitable integers } s \text{ and } t,$$

and so

$$b = bsc + btm.$$

Since the final term is a multiple of m, $b \equiv (bs)c \pmod{m}$, and $x = bs$ is the required solution of the congruence. As an example, suppose we wish to solve the congruence

$$5x \equiv 4 \pmod{3}.$$

We seek integers x,y such that $5x - 4 = 3y$

$$\text{i.e. } 5x - 3y = 4.$$

The general solution of this diophantine equation is $x = 3t - 4$, $y = 5t - 8$, $t \in J$ and the smallest positive integral value of x is obtained by substituting $t = 2$, giving $x = 2$ as the solution of the congruence.

In this paper I have discussed Euclid's algorithm for finding the HCF of two positive integers. However the theory can be extended to the case of polynomial functions. If $f(x)$, $g(x)$ are polynomials over a field ϕ, then there exists a polynomial $h(x)$, unique apart from an arbitrary factor taken from ϕ such that

(i) $h(x)$ divides both $f(x)$ and $g(x)$
(ii) polynomials $F(x)$, $G(x)$ can be found such that $F(x)f(x) + G(x)g(x) = h(x)$.

I will not give the proof of this result here; the interested reader is referred to Littlewood's book [2]. The most important

application of the division algorithm for polynomials is in finding algebraic partial fractions, and the detailed theory of algebraic partial fractions will be found in Barnard and Child [3].

References.

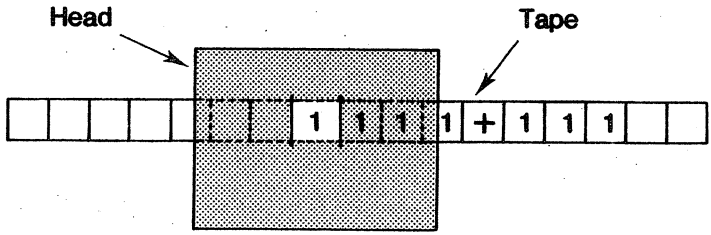
1. Allendoerfer, C.B. & Oakley, C.O.: Principles of Mathematics. McGraw-Hill, 3rd edition (Chapter 3).

2. Littlewood, D.E.: A University Algebra. Heinemann, 2nd edition (Chapters 8, 10).

3. Barnard, S. & Child, J.M.: Higher Algebra. Macmillan, 1st edition (Chapter 7).

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

MORE ON TURING MACHINES



	STATE A	STATE B
1	1. ERASE THE 1. 2. SCAN NEXT CELL ON RIGHT. 3. GO TO STATE B.	1. SCAN NEXT CELL ON RIGHT. 2. STAY IN STATE B.
+		1. ERASE THE +. 2. PRINT 1. 3. STOP.

The number 4 (represented as 1111) is to be added to the number 3 (111). Check that this Turing machine, programmed as above, does this. Assume that the machine is initially in State A, and that the reading head is situated as shown in the diagram.

Can you now complete the program to remove these restrictions? What if the number 1 were represented, as Professor Crossley suggests, as 11, 2 as 111, etc.? How would you then modify the program?

Based on an example in *Scientific American*, July, 1971.

THE POISSON APPROXIMATION TO BINOMIAL

T.C. Brown, Monash University†

The binomial distribution arises frequently in probability and statistics. As an example, suppose that a random sample of 1000 people is chosen from a population in which 0·1% of people have a rare disease. If the sampling is done with replacement, then the probability that j people in the sample have the disease is given by the binomial probability

$$\binom{1000}{j}(0\cdot001)^j(0\cdot999)^{1000-j}$$

where j could be $0,1,2,\ldots,1000$. The expected number of disease victims in the sample would be $1000 \times 0\cdot01 = 1$. If j is at all large, it is tedious to calculate this probability exactly. Instead, we could approximate it by the corresponding probability from the Poisson distribution of mean 1. This is

$$e^{-1}\, 1^j/j! = (e(j!))^{-1}$$

and is considerably easier to calculate. However, some readers may have calculators that will compute binomial probabilities exactly and they may wonder about the relevance of the Poisson approximation. These readers may care to try out the following problem on their binomial calculator. Suppose a room has 10^{26} particles in it and that each particle has probability 10^{-12} of being 'special'. What is the probability of having less than 10^6 special particles in the room? (For solution, see later.)

In this article, the *quality* of the Poisson approximation to the binomial will be examined. Let us first recall the general approximation. Take the non-negative integers $\{0,1,2,\ldots\}$ as sample space. Let A be an event, so that $A \subseteq \{0,1,2,\ldots\}$. The binomial probability of A with parameters n and p is $B(A)$ given by

$$B(A) = \sum_{j\in A} \binom{n}{j} p^j (1-p)^{n-j} .$$

†Now at the University of Melbourne.

In the first example, $B(A)$ is the probability that the number of disease victims lies in A if $n = 1000$ and $p = 0{\cdot}001$. The approximation to $B(A)$ using the Poisson distribution with mean np (coinciding with the mean of the binomial distribution) is

$$Po(A) = \sum_{j \in A} e^{-np}(np)^j/j! \ .$$

In the second example above $A = \{0,1,\ldots,10^6-1\}$, $n = 10^{26}$ and $p = 10^{-12}$, so that $np = 10^{14}$.

Readers may be familiar with the advice that

'the Poisson approximation may be used when n is large, p is small and np is moderate'.

The implication of this advice would appear to be that in these circumstances

$$|Po(A) - B(A)|$$

will be small for all events A. In fact, this implication is true, but overly cautious, the circumstances in which the approximation is appropriate are much wider.

But let us first look at the example in which $n = 1000$ and $p = 0{\cdot}001$. In Table 1 the individual Binomial and Poisson probabilities are listed.

Table I

Binomial and Poisson probabilities, $n = 1000$, $p = 0{\cdot}001$ to 5 decimal places

j	Binomial	Poisson	Difference
0	0·36770	0·36788	-0·00018
1	0·36806	0·36788	+0·00018
2	0·18403	0·18394	+0·00009
3	0·06128	0·06131	-0·00003
4	0·01529	0·01533	-0·00004
5	0·00305	0·00307	-0·00002
6	0·00051	0·00051	$<10^{-5}$
7	0·00007	0·00007	$<10^{-5}$
8	0·00001	0·00001	$<10^{-5}$
9	$<10^{-5}$	$<10^{-5}$	$<10^{-5}$
.	.	.	.
.	.	.	.
total	1·00000	1·00000	0·000000

For some values of j, namely $j = 0,3,4$, and 5, the Poisson probability *overestimates* the binomial probability. On the other hand, for $j = 1$ and 2 the Poisson probability underestimates the binomial probability, which for all other j the two probabilities coincide to 5 decimal places. In general, let A_0 be the event consisting of those j for which the Poisson

probability is an overestimate and A_u be the event consisting of those j for which either the Poisson probability is an underestimate or both are equal. So, in the example, $A_0 \supseteq \{0,3,4,5\}$ and $A_u \supseteq \{1,2\}$. We do not know whether $6,7,8,9,\ldots,1000$ are in A_u or A_0 but certainly $1001,1002,\ldots$ are in A_0 because $B\{1001,1002,\ldots\} = 0$. Notice that

$$\begin{aligned} B\{1,2\} - Po\{1,2\} &= \text{sum of positive differences in Table 1} \\ &= 0{\cdot}00018 + 0{\cdot}00009 \\ &= 0{\cdot}00027 \end{aligned}$$

and

$$Po\{0,3,4,5\} - B\{0,3,4,5\} = 0{\cdot}00027.$$

In general, since

$$Po(A_u) + Po(A_0) = B(A_u) + B(A_0) = 1,$$

we have

$$Po(A_0) - B(A_0) = B(A_u) - Po(A_u) \quad . \tag{1}$$

Equation (1) is more important than it might seem at first sight. From it we may deduce that $Po(A_0) - B(A_0)$ and $B(A_u) - Po(A_u)$ are events A for which $|B(A) - Po(A)|$ is maximal over all events A. To see this, suppose that A is an event for which $B(A) > Po(A)$. For concreteness, let us take $A = \{1,3\}$ in the first example. Then

$$\begin{aligned} |B(A) - Po(A)| &= 0{\cdot}00018 - 0{\cdot}00003 \\ &< 0{\cdot}00018 \\ &< 0{\cdot}00018 + 0{\cdot}0009 \\ &= B(A_u) + Po(A_u) \, . \end{aligned}$$

Thus, in general, we increase $B(A) - Po(A)$ by adding back the negative differences and the result, since it omits some terms of $B(A_u) - Po(A_u)$, is still smaller than $B(A_u) - Po(A_u)$. A similar argument shows that $Po(A) - B(A) \leqslant Po(A_0) - B(A_0)$ if $Po(A) \geqslant B(A)$. Thus equation (1) tells us that for all A

$$|B(A) - Po(A)| \leqslant B(A_u) - Po(A_u) \tag{2}$$

which is 0·00027 in the example.

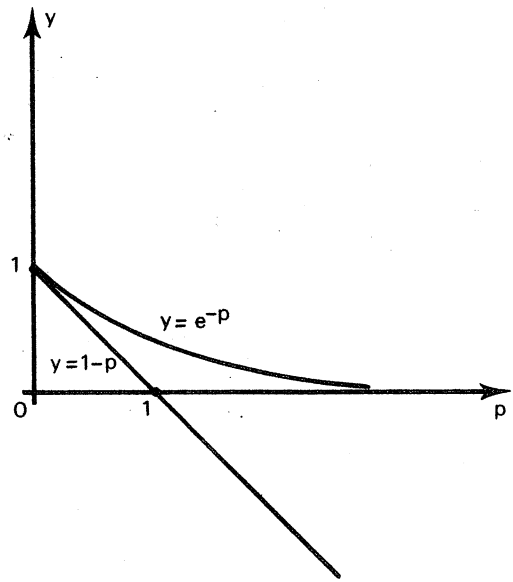
The problem then is to try to find a general *formula* for $B(A_u) - Po(A_u)$ in terms of n and p; if you are at all successful then you deserve great praise, for this is a very hard problem. Using quite advanced mathematics, general upper *bounds* for $B(A_u) - Po(A_u)$ can be found and we mention two of these shortly. However, in one general case, it is possible to find $B(A_u) - Po(A_u)$ exactly.

This is the case for which $n = 1$. The crucial point is that for $p > 0$

$$1 - p < e^{-p} \tag{3}$$

an identity which is illustrated in Figure 1.

Figure 1.



Thus $0 \in A_0$ and since $B\{2,3,4,\ldots\} = 0$, $\{2,3,4,\ldots\} \subseteq A_0$ and $A_u = \{1\}$. Thus, for any A, from equation (2)

$$|B(A) - P_0(A)| \leqslant B\{1\} - P_0\{1\}$$

$$= p(1 - e^{-p}).$$

It may not appear very impressive that we have been able to find $B(A_u) - Po(A_u)$ in this case; p and $1 - p$ are much simpler than $e^{-p}, pe^{-p}, \ldots$. However, the above calculation is a key step in showing that for *all* n

$$B(A_u) - Po(A_u) \leqslant np(1 - e^{-p}) < np^2 \qquad (4)$$

by (3). This is a special case of a more general result I proved recently (*Am. Math. Monthly*, Feb. 1984). Its implications are clear. Since $np^2 = (np).p$, Equations (2) and (4) tell us that no matter what event A is chosen, the Poisson approximation is always accurate if

'p is small and np is moderate'.

Thus, we can already see that the advice given before is cautious because n *need not be large* in order that the approximation be accurate.

Unfortunately, the bound of (4) is not always adequate; in the second example, we have $np^2 = 10^2$ and it is hardly interesting to know that the difference in two probabilities is less than a hundred. However, a deeper analysis of $B(A_u) - Po(A_u)$ shows that it is always bounded by $p/\sqrt{1 - p}$. Hence, the best general advice is

'the Poisson approximation may be used if p is small'.

In particular, the approximation will be excellent in the second example, as $p/\sqrt{1 - p} < \sqrt{2} \times 10^{-12}$. Thus with an error of at most $\sqrt{2} \times 10^{-12}$ the probability of less than a million particles in the room is

$$P_0\{0,1,\ldots,10^6-1\} = \sum_{j=0}^{10^6-1} e^{-10^{14}} \left(10^{14}\right)^j / j!$$

$$< 10^6 \times e^{-10^{14}} \left(10^{14}\right)^6$$

replacing each term in the sum by the (much larger) constant term $e^{-10^{14}}\left(10^{14}\right)^6$. It is straightforward therefore to see that the required probability is zero to many decimal places!

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

THE POISSON DISTRIBUTION APPLIED

A famous and often quoted historical example is that of Bortkiewicz, who discovered that the number of men kicked to death by a horse in a Prussian army corps each year closely followed the Poisson distribution.

N.T.J. Bailey, *Statistical Methods in Biology*, 1959.

LETTER TO THE EDITOR

A MORE COMPLETE RESULT

Problem 8.3.2 naturally suggests the following question: Of all triangles with sides of integral length, which ones have a perimeter equal to the area? We settle this question by showing that the only such triangles are those with side-lengths (5,12,13), (6,8,10), (6,25,29), (7,15,20), (9,10,17).

Let a,b,c be integers which can be the sides of a triangle. Let $P = a + b + c$. Heron's formula for the area of a triangle (*Function Vol.*8, *Part* 1) then gives, if the perimeter equals the area:

$$P = \left\{\frac{P}{2}\left(\frac{P}{2} - a\right)\left(\frac{P}{2} - b\right)\left(\frac{P}{2} - c\right)\right\}^{\frac{1}{2}}$$

or

$$16P = (P - 2a)(P - 2b)(P - 2c). \qquad (1)$$

Now if P were odd, all the factors on the right would be odd and so would be their product. But this cannot be as $16P$ is even. Thus P is also even. If then

$$\alpha = \tfrac{1}{2}(P - 2a),\ \beta = \tfrac{1}{2}(P - 2b),\ \gamma = \tfrac{1}{2}(P - 2c),$$

these expressions are all integral. Furthermore, we may assume without loss of generality that $\alpha \geqslant \beta \geqslant \gamma$.

Equation (1) now becomes

$$4(\alpha + \beta + \gamma) = \alpha\beta\gamma. \qquad (2)$$

Now suppose $\gamma \geqslant 4$. Then, by Equation (2), as $\alpha\beta\gamma \geqslant 4\alpha\beta$,

$$4(\alpha + \beta + \gamma) \geqslant 4\alpha\beta$$

or

$$\gamma \geqslant \alpha\beta - (\alpha + \beta) = (\alpha - 1)(\beta - 1) - 1.$$

Thus

$$\gamma + 1 \geqslant (\alpha - 1)(\beta - 1).$$

But $\alpha \geqslant \beta \geqslant \gamma$, and so

$$\gamma + 1 \geqslant (\gamma - 1)^2$$

or

$$\gamma \leqslant 3$$

contradicting our assumption. Thus $\gamma < 4$ and the possible values are 1,2,3.

Return now to Equation (2) and write it as

$$4\gamma(\alpha + \beta + \gamma) = \alpha\beta\gamma^2$$

or

$$\alpha\beta\gamma^2 - 4(\alpha + \beta)\gamma + 16 = 4\gamma^2 + 16$$

or

$$(\gamma\alpha - 4)(\gamma\beta - 4) = 4(\gamma^2 + 4). \qquad (3)$$

We investigate first the case $\gamma = 3$. If now α were 3, $\gamma\alpha - 4$ would be 5 which does not divide $4(3^2 + 4) = 52$. Thus $\alpha \neq 3$ and $\alpha \geqslant 4$, $\beta \geqslant 4$. But then $(3\alpha - 4)(3\beta - 4) \geqslant (3\beta - 4)^2 \geqslant 8^2 = 64 > 52$ and so there is no solution if $\gamma = 3$.

If now $\gamma = 2$, Equation (3) becomes

$$(\alpha - 2)(\beta - 2) = 8$$

which implies that $\alpha = 10$, $\beta = 3$ or $\alpha = 6$, $\beta = 4$.

Finally if $\gamma = 1$, Equation (3) becomes

$$(\alpha - 4)(\beta - 4) = 20,$$

which implies that $\alpha = 24$, $\beta = 5$ or $\alpha = 14$, $\beta = 6$ or $\alpha = 9$, $\beta = 8$.

But from the definitions of α,β,γ we have $a = \beta + \gamma$, $b = \gamma + \alpha$, $c = \alpha + \beta$ and so the result follows.

Colin Wratten
20 Wilson Street, Highett.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

MATHEMATICS MODELS REALITY

The essentials of the abstract general truth in a physical situation can be described in mathematical terms incomparably better than in other ways. This description is unlike an exact photographic reproduction of reality. It is in no sense a record or a moving picture. A physical law mathematically described reveals certain general essentials, not just any one particular sequence of events. But it can be used to describe and predict actual physical events.

Francis Bitter, *Mathematical Aspects of Physics*, 1963.

PROBLEM SECTION

We here give solutions to many of the outstanding problems. Some of these were quite difficult.

SOLUTION TO PROBLEM 8.2.1.

This concerned the packing of tubes into hexagonal arrays. Such arrays contain 1,7,19,37,61,91,... tubes. We asked what was the 69th number ending in 69 and belonging to this sequence.

David Shaw of Geelong West Technical School sent us a detailed solution which we summarise here. He first found the nth term in the sequence to be

$$t_n = 3n^2 - 3n + 1.$$

Then using congruences (see recent *Perdix* columns), he wrote

$$t_n \equiv 69 \pmod{100},$$

an equation that reduces to

$$n^2 - n - 56 = 100t,$$

where t is integral. Then

$$n = \tfrac{1}{2}(1 \pm 5\sqrt{9 + 16t})$$

and so

$$9 + 16t = N^2,$$

where N is integral. So now

$$N^2 \equiv 9 \pmod{16}.$$

This congruence is readily solved. We find

$$N \equiv 3,5,11,13 \pmod{16}.$$

Thus

$$N = 16K + 3,\ 16K + 5,\ 16K + 11,\ 16K + 13,$$

where K is integral. Then

$$n = 40K + 8,\ 40K + 13,\ 40K + 28,\ 40K + 33$$

for $K = 0,1,2,3,\ldots$. The 69th member of this sequence is $40 \times 17 + 8 = 688$, and $t_{688} = 1417969$.

SOLUTION TO PROBLEM 8,2,2,

This problem asked for the circumradius of each of the five regular solids: the tetrahedron, the cube, the octohedron, the dodecahedron and the icosahedron.

No one sent in a solution, even though the first three cases, especially the octohedron, are not difficult. Take, in each case, the edge to be 1. Then the answers are, respectively,

$$\sqrt{3}/2\sqrt{2},\ \sqrt{3}/2,\ 1/\sqrt{2},\ \sqrt{3}/(\sqrt{5}-1),\ 1\sqrt{(2-2/\sqrt{5})}.$$

The problem is fully discussed in H.S.M. Coxeter's *Introduction to Geometry* (Wiley, 1961), Chapter 10, and we refer readers to this account. An article on the icosahedron will shortly appear in *Function*. This will show this case very clearly.

SOLUTION TO PROBLEM 8,2,3,

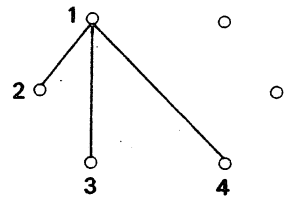
The problem read:

(a) Show that in any party of six or more people, there is at least one set of three people all acquainted with each other or at least one set of three people no two of whom are acquainted.

(b) In a party of six people must there be either four mutual acquaintances or four mutual strangers?

It helps to put the problem in terms of *graph theory* (see Jacqueline Wong's article in *Function, Vol.*8, *Part* 3). Represent each person by a point and acquaintance by a line between two points. The graph G then consists of 6 points and some subset of the 15 possible connections between them. Draw also a graph $\overline{G}$ consisting of the 6 points and precisely those lines not in G. Then (a) says that either G or $\overline{G}$ contains a triangle of lines.

Consider one particular person and the point (1) representing him/her. Either this point connects to 3 or more others (in G) or it doesn't, in which case it will connect in $\overline{G}$. Suppose the connections occur in G.



Call these points 2,3,4. Then if no connections exist between these points in G they form a triangle in $\overline{G}$. But if they allow a connection (say 2-3) then a triangle (1-2-3) is formed.

The answer to part (b) is "no". To see this, consider the case in which G consists of two disjoint triangles. Then every person is acquainted with exactly two other people.

SOLUTION TO PROBLEM 8.3.1.

The problem read:

> In the year 1949, a man turned 67. His four sons turned 37, 31, 29, 23 respectively. All five reached prime age in a prime year. It was the golden year for that family. When was or will be their next golden year?

D. Halprin (P.O. Box 23, North Carlton) found the ages were 97, 67, 61, 59, 53 (all prime) in 1979 (also a prime). David Dyte (Year 10, Scotch College) found that in the prime year 1913, the father was 31, and his only son alive at that time 1 (almost a prime). He also notes that in the prime year 1889, the father was 7 and the sons could be thought of as being -23, -29, -31, -37, the exact negatives of their present ages and so also prime!

SOLUTION TO PROBLEM 8.3.2.

Are there Pythagorean triangles whose perimeters equal their areas?

Colin Wratten (12 Wilson Street, Highett) sent in two proofs that the only cases are 5, 12, 13 and 6, 8, 10. Here is one of them.

Let a,b be the legs and c the hypotenuse of the triangle. Then the area is $ab/2$ and the perimeter is $a + b + c$, where $c^2 = a^2 + b^2$ and a,b,c are all integers.

It is well-known (see e.g., *Function, Vol.3, Part 3*) that we now need $a = 2rst$, $b = r(s^2 - t^2)$, $c = r(s^2 + t^2)$ where r,s,t are positive integers and $s > t$. Applying these formulae to the equation $ab/2 = a + b + c$ we find

$$r(2st + s^2 - t^2 + s^2 + t^2) = r^2st(s^2 - t^2),$$

which simplifies to

$$rt(s - t) = 2.$$

This equation has three solutions in integers

$$r = t = 1,\ s = 3;\ r = 1,\ t = 2,\ s = 3;\ r = 2,\ t = 1,\ s = 2$$

and these give respectively

$$a = 6,\ b = 8,\ c = 10;\ a = 12,\ b = 5,\ c = 13;\ a = 8,\ b = 6,\ c = 10$$

and the first and third of these are the same.

SOLUTION TO PROBLEM 8.3.3.

> Toss a fair coin 100 times and keep a tally of progressive numbers of heads and tails. How many times (on average) will the lead change from one to the other?

Number the tosses $1,2,3,\ldots,100$. The progressive totals can be equal (say when there have been k heads and k tails) after an *even* number of tosses (say $2k$ tosses). The probability that they *are* equal after $2k$ tosses is the binomial probability

$$p_k = \binom{2k}{k}\left(\tfrac{1}{2}\right)^k\left(\tfrac{1}{2}\right)^k = \binom{2k}{k}\left(\tfrac{1}{2}\right)^{2k} .$$

After the next $(2k + 1)$ toss, the lead *may* change from what it used to be, with probability $\frac{1}{2}$ (if heads used to be ahead, then $\frac{1}{2}$ is the chance that a tail will be tossed on toss $2k + 1$, and similarly with heads and tails interchanged).

So the probability that the lead *will* change on toss $2k + 1$ is $\frac{1}{2}p_k$. The expected number of changes in lead on toss $2k + 1$ is $1 \times \frac{1}{2}p_k + 0 \times (1 - \frac{1}{2}p_k) = \frac{1}{2}p_k$ because there can either be one, or none, changes of lead on toss $2k + 1$. The total expected number of changes of lead over all the (odd-numbered) tosses is

$$\tfrac{1}{2}p_1 + \tfrac{1}{2}p_2 + \tfrac{1}{2}p_3 + \ldots + \tfrac{1}{2}p_{49} . \qquad (1)$$

To calculate this note that $p_1 = \binom{2}{1}\left(\frac{1}{2}\right)^2 = \frac{1}{2}$; and it is easy to see in general that $p_k = \left(1 - \frac{1}{2k}\right)p_{k-1}$. Then a calculator or computer can be used to add up (1). The answer is about 3·48.

SOLUTION TO PROBLEM 8.3.4.

Is there a cuboid whose sides and diagonals all have integral lengths?

Yes. The smallest has sides 44, 117, 240. This discovery is credited to the 18th century mathematician Leonhard Euler; see *Scientific American*, July 1970, p.118.

SOLUTION TO PROBLEM 8.3.5.

In a common type of logic-puzzle, we are confronted with two categories of person: those who always lie and those who always tell the truth. A traveller reached a land in which the inhabitants all fell into two such classes and, seeing a house, he wished to ascertain whether it was an inn where he could spend the night. Approaching two people, he asked the first, but received a cryptic reply, insufficient to give him his answer. He addressed exactly the same question to the second person and received exactly the same reply. He then knew the house to be an inn.

What was the cryptic reply?

David Dyte writes:

My solution is this: "It isn't an inn at all, but he would say that it is." (You said cryptic!)

To test this solution, the feasibility of the three possible combinations of the two men must be tested. These are: True True; True False; False False.

1. True True. This combination is impossible, as both men, with knowledge of each other's honesty, could not reply in contradiction of each other.

2. True False. This combination is also impossible, because, if one tells the truth, it must be not an inn, *but* his falsehooding counterpart says it isn't also, creating paradox and impossibility.

3. False False. This combination is possible, if both say it isn't an inn and lie about the other's reply, then it must be an inn.

Q.E.D.

By deduction, the traveller works out it must be an inn.

This solution is simpler (and hence better) than that published in *The Mathematical Gazette* where we found the problem.

SOLUTION TO PROBLEM 8.4.1.

This asked for the sum of a continued fraction whose numerators were all 1 and whose denominators all $2i$.

To solve such problems merely note that if x is the value, then

$$x = \frac{1}{2i + x} .$$

So $$x^2 + 2ix - 1 = 0$$

i.e. $$(x + i)^2 = 0$$

or $$x = -i$$

as given.

SOLUTION TO PROBLEM 8.4.3.

A regular octagon, with all its diagonals, is drawn. How many points of (interior) intersection are found?

By drawing a reasonably accurate diagram and counting, we find the answer 49. Does any reader know of a reasonably elementary theoretical approach?

No pattern seems to be discernible: if n is the number of vertices and N the number of intersections, we find

n	3	4	5	6	7	8
N	0	1	5	1	35	49

which seems to lead nowhere.

Our problems for the long vacation all come from Colin Wratten.

PROBLEM 8.5.1.

Let r, x, y and z be real or complex variables. Show that:

(i) $y \propto x$ if y changes by a factor of r whenever x changes by a factor r. [Assume y is known to be a function of x.]

(ii) $z \propto xy$ if $z \propto x$ for each fixed y and $z \propto y$ for each fixed x. [Assume z is known to be a function of both x and y, i.e., to each suitable x and y, there corresponds just one z.]

PROBLEM 8.5.2.

Let $A = \sqrt{5} + \sqrt{22 + 2\sqrt{5}}$ and
$B = \sqrt{11 + 2\sqrt{29}} + \sqrt{16 - 2\sqrt{29} + 2\sqrt{55 - 10\sqrt{29}}}$. Prove that $A = B$.

PROBLEM 8.5.3

A particle is projected vertically into the air; it ascends to a certain height and then descends to the point of projection, all in the same straight line. Taking air-resistance into account, show that the initial (projection) speed is greater then the final (impact) speed and that the ascent time (the time to reach maximum height) is less than the descent time.

PERDIX

We now have the full results for the 1984 International Mathematical Olympiad. Australia's creditable performance indicates a steady improvement in our position, but, as you can see, there is still a long way to go.

Pos.	Country	Marks (Poss. max.252.)	Pos.	Country	Marks
1	Russia	235	18	Brazil	92
2	Bulgaria	203	19	Greece	88
3	Romania	109	20	Canada	83
4	U.S.A.	195	21	Colombia	80
4	Hungary	195	22	Cuba	67
6	Great Britain	169	23	Belgium	56
7	Vietnam	162	23	Morocco	56
8	East Germany	161	25	Sweden	53
9	West Germany	150	26	Cyprus	47
10	Mongolia	146	27	Spain	43
11	Poland	140	28	Algeria	36
12	France	126	29	Finland	31
13	Czechoslovakia	125	30	Tunisia	29
14	Yugoslavia	105	31	Norway	24
15	Australia	103	32	Luxembourg	22
16	Austria	97	33	Kuwait	9
17	Holland	93	34	Italy	0

These were the questions set.

First day, 4 July, 1984.

1. Prove that

$$0 \leqslant yz + zx + xy - 2xyz \leqslant \frac{7}{27},$$

where x, y, z are non-negative real numbers for which $x + y + z = 1$.

2. Find one pair of positive integers a, b such that:

(1) $ab(a + b)$ is not divisible by 7,
(2) $(a + b)^7 - a^7 - b^7$ is divisible by 7^7.

Justify your answer.

3. In the plane two different points $0, A$ are given. For each point X of the plane, other than 0, denote by $a(X)$ the measure of the angle between $0A$ and $0X$ in radians, counterclockwise from $0A$ $(0 \leqslant a(X) < 2\pi)$. Let $C(X)$ be the circle with centre 0 and radius of length $0X + \frac{a(X)}{0X}$. Each point of the plane is colored by one of a finite number of colors. Prove that there exists a point Y for which $a(Y) > 0$ such that its color appears on the circumference of the circle $C(Y)$.

Time allowed: $4\frac{1}{2}$ hours. Each question is worth 7 points.

Second day, 5 July, 1984.

4. Let $ABCD$ be a convex quadrilateral such that the line CD is a tangent to the circle on AB as diameter. Prove that the line AB is a tangent to the circle on CD as diameter if and only if the lines BC and AD are parallel.

5. Let d be the sum of the lengths of all the diagonals of a plane convex polygon with n vertices $(n > 3)$, and let p be its perimeter.

Prove that

$$n - 3 < \frac{2d}{p} < \left[\frac{n}{2}\right]\left[\frac{n+1}{2}\right] - 2.$$

($[x]$ denotes the greatest integer not exceeding x.)

6. Let a, b, c, d be odd integers such that $0 < a < b < c < d$ and $ad = bc$.

Prove that if $a + d = 2^k$, $b + c = 2^m$ for some integers k and m, then $a = 1$.

Time allowed $4\frac{1}{2}$ hours. Each question is worth 7 points.

∞ ∞ ∞ ∞

We now conclude our discussion of the problems in Vol.8 Part 3 by solving Problem 3 of that issue.

PROBLEM 3. (Twelfth International Olympiad, 1970, problem 4)

Find the set of all positive integers n with the property that the set $\{n,n+1,n+2,n+3,n+4,n+5\}$ can be partitioned into two sets such that the product of the numbers in one set equals the product of the numbers in the other set.

Solution

We shall assume that you know (or will accept) that any positive integer is the product of uniquely determined prime numbers, each occurring as a factor a unique number of times. For example $2^3 \times 5^2 \times 7$ is the only way of expressing 1400 as a product of prime numbers.

When the set $A = \{n,n+1,n+2,n+3,n+4,n+5\}$ is partitioned into two sets such that the product of those in one set equals the product of those in the other set, then each of these products equals the same product of prime numbers. Hence any prime that divides one product must divide the other. So each prime p dividing any one of these numbers $n,n+1,\ldots,n+5$, must divide another of the numbers.

Now if a prime p divides an integer k, then the next largest integer that p divides is $k + p$. Hence the only primes that can divide two of the members of the set of numbers A are 2, 3, and 5.

Suppose 5 is a divisor, so that 5 divides k and $k + 5$, where k is a member of A. This can happen only if $k = n$. In this event, $n + 1$, $n + 2$, $n + 3$, and $n + 4$ have to be products of powers of 2 and 3. But this is impossible for four consecutive integers, because (a) if $n + 1$ is divisible by both 2 and 3 then $n + 2$ is divisible by neither; (b) if $n + 1$ is divisible by 2 but not by 3, then $n + 2$ is a power of 3 and hence $n + 4$ is divisible by neither 2 nor 3 (it is congruent to 1 mod 2 and congruent to 2 mod 3); (b) if $n + 1$ is divisible by 3 but not by 2, then $n + 2$ is a power of 2, whence $n + 3$ is not divisible by either 2 or 3. Thus the assumption that 5 is a divisor of any member of A leads to a contradiction in all cases.

Hence the only possible prime factors of each of n, $n + 1$, $n + 2$, $n + 3$, $n + 4$, $n + 5$ are 2 and 3. But, in the previous paragraph we have shown that no four consecutive integers can be such that their only prime factors are 2 or 3. Hence we are again led to a contradiction.

Hence there are no positive integers n satisfying the stated conditions. The set we have to find is the empty set.

* * * * * * *

The methods we have developed to solve problems 1, 2, and 3 should now enable you to have an effective attack on problem 4 of Volume 8, Part 3. Have a shot if you have not yet managed to solve it.

Here are some further problems using the same circle of ideas.

PROBLEM 5 (First Hungarian Eötvös Competition, 1894, problem 1)

Prove that the expressions $2x + 3y$ *and* $9x \times 5y$ *are divisible by* 17 *for the same set of integral values of* x *and* y.

PROBLEM 6 (Eötvös Competition, 1898, problem 1)

Determine all positive integers n *for which* $2^n + 1$ *is divisible by* 3.

PROBLEM 7 (Eötvös Competition, 1899, problem 3)

Prove that, for any natural number n, *the expression*

$$A = (2903)^n - (803)^n - (464)^n + (261)^n$$

is divisible by 1897.

PROBLEM 8 (Eötvös Competition, 1900, problem 1)

Let a,b,c,d *be fixed integers with* d *not divisible by* 5 *Assume that* m *is an integer for which*

$$am^3 + bm^2 + cm + d$$

is divisible by 5. *Prove that there exists an integer* n *for which*

$$dn^3 + cn^2 + bn + a$$

is also divisible by 5.

DO NOT READ ON UNTIL YOU HAVE CAREFULLY CONSIDERED THESE PROBLEMS.

Solutions

PROBLEM 4. *Let* m *be an odd positive integer. Show that there is a positive integer* k *such that* m *divides* $2^k - 1$. (*Function, Vol.*8, *Part* 3, inside back cover.)

Instead of solving this problem we shall establish the following important result, from which a solution to the problem follows as a special case.

RESULT 3. *Let* m *and* n *be positive integers that are co-prime, i.e. such that their highest common factor is* 1. *Then there exists a positive integer* k *such that* m *divides* $n^k - 1$.

Proof. A hint of how to prove this is suggested by the solution, in the last issue, of Problem 2, and the subsequent remarks, including Result 1 and Result 2, on modular arithmetic. What was shown there was that the remainders, i.e. residues, on division by 7, of the powers $2, 2^2, 2^3, 2^4, \ldots$, repeated themselves in cycles. The same happens to the residues of $n, n^2, n^3, \ldots$, on

division by m. We need slightly less than this to establish Result 3: all we need is that two remainders are the same.

Let us assume that $n > 1$. If $n = 1$, then $n^k - 1 = 0$ and, since $m \times 0 = 0$, m divides $n^k - 1$. So the result is true when $n = 1$.

When $n > 1$, the sequence $n, n^2, n^3, \ldots$ is an infinite sequence, but, on division by m, the residues we get can only take a finite number of values, namely an integer r such that $0 \leqslant r \leqslant m - 1$. Hence the residues of two distinct powers of n are the same, i.e. there exist positive integers, k and ℓ, say, such that

$$n^{k+\ell} \equiv n^{\ell} \pmod{m}.$$

Then

$$n^{k+\ell} - n^{\ell} = qm,$$

for some integer q, i.e.

$$n^{\ell}(n^k - 1) = qm.$$

Since m and n are co-prime, no factor of m can divide n^{ℓ}. Hence m divides $n^k - 1$; which is what we had to show.

Remarks. Taking into account that there are only m possible distinct residues, modulo m, and observing that, since n and m are co-prime, no power of n gives residue 0, it follows that the longest sequence $n^a, n^{a+1}, n^{a+2}, \ldots$, of powers of n, that give residues modulo m that are all distinct, is of length $m - 1$: there must be a repetition of a previous residue at the mth term, if there has not been one already. Hence, we can sharpen the above argument, used for the proof of Result 3, to show that ℓ and k can be chosen so that $k \leqslant m - 1$. Thus we have

RESULT 3'. *If m and n are co-prime integers, then there is a positive integer k, less than or equal to $m - 1$, such that m divides $n^k - 1$.*

UNSOLVED PROBLEM. *Find a formula, depending on m and n, to give the smallest positive k, such that m divides $n^k - 1$.*

In dealing with Mathematical Olympiad problems you are trying to solve problems that someone else has already solved. In addition to knowing that they can be solved, you know that the solutions are not too long; for, in the competition, you have only a limited time to find and write out your solutions. *Unsolved problems*, that no-one has yet solved, are quite a different kettle of fish.

The kind of argument that was used to establish Result 3, is sometimes called the *Pidgeon-hole Principle*. This states:

If you put more than m letters into at most m pidgeon-holes, then there must be two or more letters in at least one of the pidgeon-holes.

Before continuing to our next problem let us draw another

conclusion from Result 3 that is extremely useful and which we shall use shortly.

RESULT 4. *Let m and n be co-prime positive integers. Then there exist integers r and s, say, such that*

$$rm + sn = 1.$$

Proof. By Result 3, there exist a positive integer k and an integer q such that $qm = n^k - 1$. Thus

$$(-q)m + (n^{k-1})n = 1.$$

Take $r = -q$ and $s = n^{k-1}$, interpreting n^{k-1} to be 1, when $k = 1$. Then

$$rm + sn = 1,$$

as required.

PROBLEM 5 (*Function*, this issue,p.29). *Prove that the expressions $2x + 3y$ and $9x + 5y$ are divisible by 17 for the same set of integral values of x and y.*

Solution. Observe that

$$4(2x + 3y) + (9x + 5y) = 17(x + y).$$

Hence, if 17 divides $2x + 3y$ it divides

$$9x + 5y = 17(x + y) - 4(2x + 3y).$$

Similarly, if 17 divides $9x + 5y$, it divides $2x + 3y$, since 4 and 17 are co-prime.

PROBLEM 6 (*Function*, this issue p.29). *Determine all positive integers n for which $2^n + 1$ is divisible by 3.*

Solution. This problem is similar to the Olympiad problem, Problem 2, solved in the previous issue.

Observe that $2^n + 1 = 3q$ if and only if $2^n = 3(q - 1) + 2$. Hence 3 divides $2^n + 1$ if and only if $2^n \equiv 2 \pmod 3$. It is quickly checked that, if $k > 0$,

$$2^{2k} = 4^k \equiv 1^k = 1 \pmod 3,$$

and that

$$2^{2k+1} = 4^k \times 2 \equiv 2 \pmod 3$$

(use Result 2, previous issue). Hence 3 divides $2^n + 1$, with $n > 0$, if and only if n is odd.

PROBLEM 7 (*Function*, this issue p.29). *Prove that, for any natural number n, the expression*

$$A = (2903)^n - (803)^n - (464)^n + (261)^n$$

is divisible by 1897.

Before solving this problem, another well-known result, that we now prove, will help.

RESULT 5. *Let c and d be integers and let n be a positive integer. Then $c - d$ divides $c^n - d^n$.*

Proof. If $n = 1$ the result is immediate. Suppose that $n > 1$ and set

$$S = c^{n-1} + c^{n-2}d + \ldots + cd^{n-2} + d^{n-1}.$$

Then $$cS = c^n + c^{n-1}d + \ldots + c^2d^{n-2} + cd^{n-1}$$

and $$dS = \quad c^{n-1}d + \ldots + c^2d^{n-2} + cd^{n-1} + d^n.$$

Subtract, to get

$$(c - d)S = c^n - d^n,$$

and the result follows.

Solution (to Problem 7).

Factorize: $1897 = 7 \times 271$, and it is easily checked that 271 is prime.

We now look at the number A, of the problem, in two different ways. One way of looking at it will show that 7 divides A; the other way will show that 271 divides A. Since 7 and 271 are both prime, therefore $7 \times 271 = 1897$ divides A.

We have

$$A = B - C,$$

where $$B = (2903)^n - (803)^n,$$

and $$C = (464)^n - (261)^n.$$

By Result 5, $2903 - 803 = 2100$ is a factor of B, whence 7 is a factor of B, and similarly $464 - 261 = 203 (= 7 \times 29)$ is a factor of C, whence 7 is a factor of C. Since 7 divides B and C it divides $B - C = A$.

We also have

$$A = D - E,$$

where $$D = (2903)^n - (464)^n,$$

and $$E = (803)^n - (261)^n.$$

Hence, $2903 - 464 = 2439$ divides D and $803 - 261 = 542$ divides E, again using Result 5. But $2439 = 271 \times 9$ and $542 = 271 \times 2$. Hence 271 divides D and E and so divides $D - E = A$.

Hence $7 \times 271 = 1897$ divides A. The argument just given does not preclude the possibility that $A = 0$, when 1897 (and all other integers divide A). But this degenerate case cannot occur

here because, for all positive n, the first term of A is much bigger than the remaining three.

To bring Problem 7 up-to-date, to the year 1984, try the following problem.

PROBLEM 9. *Show that, for all positive integers n, the expression*

$$A = (2084)^n - (69)^n - (36)^n + 5^n$$

is divisible by 1984.

PROBLEM 10. *Devise corresponding problems in which* 1984 *is replaced by other numbers.*

There remains one problem to be solved:

PROBLEM 8 (*Function*, this issue, p.29). *Let a,b,c,d be fixed integers with d not divisible by* 5. *Assume the m is an integer for which*

$$am^3 + bm^2 + cm + d$$

is divisible by 5. *Prove that there exists an integer n for which*

$$dn^3 + cn^2 + bn + a$$

is also divisible by 5.

Solution. Since, for some integer q,

$$am^3 + bm^2 + cm + d = 5q,$$

we have

$$d = 5q - m(am^2 + bm + c).$$

Thus, if m is divisible by 5, so also is d, contrary to assumption. Hence 5 does not divide m, whence 5 and m are co-prime.

Now apply Result 4 (with m and n in that result replaced by m and 5, respectively), to obtain

$$rm + 5s = 1$$

for some integers r and s. (In Result 4, m was taken to be positive. If m is here negative, then replace it by $-m$, and then replace r by $-r$ in this equation.) Thus

$$mr \equiv 1 \pmod 5. \qquad \ldots \qquad (\alpha)$$

Hence, using Results 1 and 2 of the previous issue, we have

$$(am^3 + bm^2 + cm + d)r^3 = 5r^3q \equiv 0 \pmod 5$$

i.e.

$$a(mr)^3 + b(mr)^2r + c(mr)r^2 + dr^3 \equiv 0 \pmod 5,$$

i.e., using the congruence (α), $a + br + cr^2 + dr^3 \equiv 0 \pmod 5$.

Good hunting for further problems!