PROOF IN MATHEMATICS

('if', 'then' and 'perhaps')

P.R.Baxandall

W.S.Brown

G.St.C.Rose

F.R.Watson

An Occasional Publication of the

Institute of Education, University of Keele.

Proof in Mathematics ('If', 'then' and 'perhaps')

A collection of material illustrating the nature and variety of the idea of proof in mathematics.

P.R. Baxandall	University of Keele
W.S. Brown	Manchester Polytechnic
G. St.C. Rose	University of the West Indies
F.R. Watson (editor)	University of Keele

An Occasional Publication of the Institute of Education,
University of Keele,
Staffordshire, ST5 5BG.

Introduction

This booklet arose out of some work done by Bill Brown and Gerry Rose during their year at Keele. Their original has been considerably augmented and revised - I am grateful to Peter Baxandall for his suggestions and additional contributions.

We intend it as a "background book", for the use of teachers, particularly those in initial training courses. We hope that much of it may also be accessible and useful to mathematics specialists in 6th forms, and to first year undergraduates. A University course may seem at times obsessively concerned with proof ("Definition n, theorem m, (example??), definition n + 1, . . ."") yet in all this detailed discussion of particular proofs, the student may not stand back sufficiently to "see what is going on"; the trees (particular proofs) are examined in detail, the shape - and purpose - of the wood (the idea of proof) is overlooked.

Although a sixth form course may be largely concerned with techniques, it will include some proofs, and ought to provide opportunities for the development of students' powers of deductive reasoning. Few would dispute that the notion of proof is central to mathematics, yet sixth formers and undergraduates alike are often hazy about theorem and converse, proof by induction or by contradiction, counter-example and proof of impossibility. We have tried to illustrate these ideas at a fairly elementary level, so that readers will be able to see the essential principles without worrying too much about technical detail. We hope they will be stimulated to analyse the strategies of proof they encounter as they study mathematics subsequently.

Some difficult material is deferred to the Appendices, where there is a discussion of axiomatic methods, leading into the difficult area of the foundations of mathematics, and providing some indication of the power , and limitations, of mathematics. We refer also to some of the classical problems of mathematics, such as the equation of Fermat ($x^n + y^n = z^n$) and the existence of transcendental numbers. These topics are not easy. They involve ideas which may be unfamiliar to some readers and they do not generally

form part of the mainstream courses at school or degree level. Yet it seemed valuable to include them, at least in outline with references to other sources, both as useful background and to complete the picture.

As ever, mathematics cannot be absorbed passively; some illustrative exercises are provided in most sections, with solutions or hints at the end.

Many of the problems have become part of the common currency of mathematical education, but we have tried to acknowledge sources where we are aware of them, and are grateful for permission to reproduce extracts from material published elsewhere.

I should like to thank Catherine Bloor and Ann Seaton for their care and patience in typing a difficult manuscript, and Peter Baxandall and Ruth Eagle for their comments on the draft. For any errors or obscurities which remain, despite their efforts, I must accept responsibility.

F.R.W.

CONTENTS

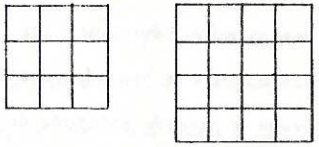
CHAPTER 1

THE ROLE OF PROOF IN MATHEMATICS

We begin with a problem:-

Find the number of squares in each of these diagrams

How many would there be on a chessboard (8 x 8)?



(i) 3 x 3 (ii) 4 x 4

(You may find it helpful to try to solve the problem yourself, before reading further).

Mathematics is concerned with numbers, with symbols, with spatial properties - but even more fundamentally it is concerned with conjecture and proof; i.e. not only with the results but how they are justified.

It is sometimes said that the essence of mathematics is problem-solving, and it is true that to be a mathematician is to be able to solve problems, as well as to know the methods-which-have-been-developed-by-others to solve problems which are the content of mathematics. "To know mathematics is to do mathematics". (Polya) Yet there are many sorts of problem - to explain how nerve impulses are transmitted through the body, why a pond seen obliquely appears shallow, to build a man-powered aeroplane. These are biological, physical, and engineering problems - what distinguishes mathematics is its total emphasis upon logical consequence - that is upon implication. The characteristic statement of mathematics is "If a, then b".

The way a gyroscope behaves is a physical fact - the explanation involves both physics (the Newtonian laws of motion which, as a matter of observation, are 'true' of the physical world), and mathematics (such logical deductions from these laws as the principle of the conservation of angular momentum).

It would give a false emphasis, however, if we were to go to the extreme and say "mathematics is logic". The study of logic in mathematical terms

(mathematical logic) has produced important contributions to the foundations of mathematics (see p. 67) but it is no longer seen as providing the sole essential basis upon which the whole superstructure of mathematics rests. Perhaps of more importance for the student - who may be content to leave discussion of the 'foundations' to the professionals - we feel this *emphasis might* encourage a passive attitude to mathematics, as the contemplation of a finished structure, rather than also involving constructive activity by the mathematician.

When learning mathematics we do exercises which usually present a clearly defined situation in which what is to be proved is explicitly stated. "Official" solutions, where these are given, are concise, direct, inevitable, with no hint of the guesses, hunches, false starts and mistakes which are likely to be involved when anyone attempts mathematics which is new to him.

Most mathematical problems - as distinct from 'practice exercises' or textbook questions - begin with a hazy, confused situation, from which emerges an idea (conjecture) - some result which is thought to be true. (It must be very strongly emphasised that this "messy" stage of thinking is typical of work in mathematics; students, accustomed to the single-minded, polished clarity of text books and lecturers, may wrongly feel that, for the expert, ideas spring, fully formed and logical, from pen to page!). An essential part of the process of problem solving, and of dealing with non-routine exercises, is arriving at such a conjecture. Perhaps the conjecture will carry with it a conviction of reasonableness. Yet the other, equally vital, step remains - it must be demonstrated, by logical argument, that its truth is a necessary consequence of the conditions of the problem. Until a proof is provided it remains only a conjecture - a useful first step, but no more.

In the "chessboard" problem, above, we find that there are 14 squares in the 3 x 3 board (9 of 1 x 1, 4 of 2 x 2, 1 of 3 x 3) and 30 squares on the 4 x 4 board (16 of 1 x 1, 9 of 2 x 2, 4 of 3 x 3, 1 of 4 x 4). Perhaps at this stage we notice a pattern; the results suggest that

for a 3 x 3 board there are $3^2 + 2^2 + 1^2 = 14$ squares

for a 4 x 4 board there are $4^2 + 3^2 + 2^2 + 1^2 = 30$ squares

"so that" for an 8 x 8 board there "will be" $8^2 + 7^2 +$ $+ 1^2 = 204$ squares, and in general,

"for an n x n board there will be $n^2 + (n-1)^2 + \ldots + 3^2 + 2^2 + 1^2$ squares".

The pattern is fairly convincing, particularly as we can extend it to the 2 x 2 case: ⊞ $4 + 1$, and with some difficulty, to the 5 x 5 case, $25 + 16 + 9 + 4 + 1$.

But can we be sure the pattern continues? We need a reason to trust the pattern. A good reason may leave us almost certain, but only a proof *gives a* completely convincing *reason.* †

We shall return to this problem later. (Ex. 3).

Exercise 1.1. On the 5 x 5 board it is easy to see why there are 25 squares of size 1 x 1; but why are there exactly 16 squares of size 2 x 2?

Another example

Consider the formula $f(n) = n^2 + n + 41$. If we work out a few values of f we obtain:-

n	0	1	2	3	4	5	6	7	8	9	10
f(n)	41	43	47	53	61	71	83	97	113	131	151

Inspection suggests two conjectures:-

(i) "The differences between successive values of f(n) increase by 2 at each step". (i.e. they are successive even numbers).

(ii) "f(n) is always prime."

(We consider these later *in more detail, but now:-*

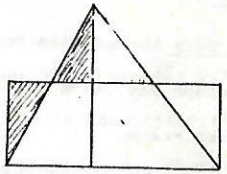
Exercise 1.2. Examine each of these conjectures. Can you think of any reason why it should be true - or false?).

We shall see very shortly that even the most plausible of conjectures may prove to be false, so that the final step, of proof, is essential.

† *Lakatos (1976) in a fascinating chapter (I), discusses how far a proof may be considered "final."*

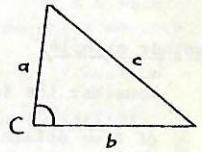
But it is a common experience to follow through the detailed steps of a proof, and yet not have a 'feel' for a theorem. The feeling of conviction in mathematics is a curious matter - it can be a powerful stimulus and a great clarifier - and can still be quite wrong! "The object of mathematical rigour is to sanction and legitimate the conquests of intuition, and there never was any other object for it." (J. Hadamard). 'Visual' proofs - considered in Ch. 3 - often carry great conviction; an example† is:-

The area of a triangle is equal to that of a rectangle on the same base and of half the height. Proof: "Look!"



The importance of a proof is not only to convince us that a theorem is true - to ensure that intuition has not played us false - but to show us why the theorem is true, and under what conditions.

For example, we know (Pythagoras) that in a triangle which is right angled at C, $a^2 + b^2 = c^2$. But where does the right angle appear in the proof? It must do so, since the result is not true for any triangle; in general $c^2 = a^2 + b^2 - 2ab \cos C$, the cosine formula.



(We must beware of the temptation to a circular argument - if we put $\cos C = 0$, since $C = 90^\circ$, we obtain Pythagoras' result. But the theorem of Pythagoras is used in proving the cosine formula!).

Exercise 1.3. Examine any proof of Pythagoras' theorem known to you. Where is the fact that $C = 90^\circ$ made use of?

Our conviction of the truth of a conjecture will be increased if we encounter more and more supporting cases - for example, the 5 x 5 case in the chess board problem, or, if we work out further values of $f(n) = n^2 + n + 41$, $f(11) = 173$, $f(12) = 197$, and see that both (i) and (ii) hold, so far. Polya (1954) gives numerous examples of how a conjecture may be tested by systematic examination of particular cases; as the weight of evidence in support of a conjecture increases, so our conviction grows that it is generally true. Yet a case may be found in which the conjecture is false - such an instance is called a counter-example. Note that whilst no amount of checking of particular cases will (in general) enable us to regard a conjecture as proved,† a single counter-example is sufficient to disprove a conjecture.

† From a Hindu source, 16th century, quoted by Popp (1974).

Examples:-

(i) Fermat conjectured that every number F_n of the form $2^m + 1$, where $m = 2^n$, is a prime number.

We examine the first few cases:-

$n = 0$	$F_0 = 2^1 + 1$	$=$	3
$n = 1$	$F_1 = 2^2 + 1$	$=$	5
$n = 2$	$F_2 = 2^4 + 1$	$=$	17
$n = 3$	$F_3 = 2^8 + 1$	$=$	257
$n = 4$	$F_4 = 2^{16} + 1$	$=$	65537

In all these cases, F_n is prime, so that our belief in the conjecture is strengthened - yet, as Euler showed, $F_5 = 2^{32} + 1$ is divisible by 641 - and so the conjecture is disproved by this single counter-example.

(ii) Put $n = 41$ in the formula $f(n) = n^2 + n + 41$.

The first of our conjectures about this formula (p.3), can be proved true, using the ideas of differences, p.49, (and see below). The second one is supported by the cases $n = 0, 1, \ldots 39$ - but fails for $n = 40$, as well as $n = 41$.

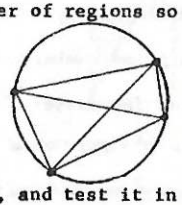
Exercise 2.

2.1. Let $f(n) = n^2 + n + 41$. Work out $f(n + 1) - f(n)$. Show the result is always an even number. Which one?

† But see "proof by exhaustion", p.32

2.2. Show that no polynomial expression in one variable x, with integer coefficients, can take <u>only</u> prime values as x takes integer values, as follows:- Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ where the a_i are integers. Let b, k be any integers, and put $c = b + k.f(b)$. Then f(c) has f(b) as a factor. (As an instance, $f(n) = n^2 + n + 41$, b = 1 gives f(b) = 43 and f(1 + 43k) is a multiple of 43). †

2.3. On the circumference of a circle, n points are marked, and all possible chords joining pairs of points are drawn. Let R_n be the maximum number of regions so formed inside the circle, *ie. when no three chords are concurrent.*

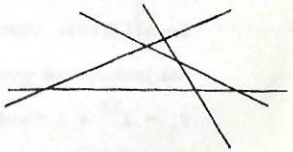


N	2	3	4	...
R_n	2	4	8	...

Make a conjecture about R_n, and test it in the cases n = 5, n = 6.

2.4. A set of n straight lines is drawn in general position in the plane (no 3 concurrent, no 2 parallel). Let R_n be the number of regions (bounded or unbounded) so formed.

N	1	2	3	4	...
R_n	2	4	7	11	...



Make a conjecture about R_n and test it in the cases n = 5, n = 6.

(Some further counter-examples are given in Appendix IIID, p. 96.)

We should not belittle the value of formulating conjectures and attempting to refute them by testing them in a variety of instances - which may prove to be confirming instances. These all help to give us the feel of the problem, and if no counter-examples are found, we shall be more convinced of the truth of a conjecture and thus more motivated to seek a proof. There is

(†) See Stewart (1975), p. 296, for a reference to a polynomial in 23 variables which produces (exactly) all the primes when positive integers are substituted.

not much point in setting out to prove a conjecture if a simple counter-example may easily be found! (e.g. "$n^3 - n$ is a multiple of 3" may be verified for n = 1, 2, 3, 4, ... ; "$n^4 - n$ is a multiple of 4" <u>fails</u> for the case n = 2). Even when an established theorem, part of the accepted structure of mathematics, is newly encountered, there is still value in similarly testing instances of it so as to understand its application; this is likely to give a clearer understanding of the details of the proof.

"When you have satisfied yourself that the theorem is true, you start proving it" Polya (1954), p.76.

<u>Exercise 3</u>. Find with proof an expression for the number of squares on an n x n chess board.

CHAPTER 2

Logical reasoning: the idea of implication

The reasoning used in a mathematical proof must be logical; that which we use in everyday affairs is often illogical. The reasons for this are varied. Sometimes the illogicality is the result of a mistake: "If he is a very learned man, I will not be able to understand what he says", or of deliberate deception - a handsome athletic male, surrounded by beautiful women, is smoking Brand-X cigarette, or wearing a suit from Messrs. Y, or is said to vote for party Z.

In the first case, an incomprehensible paragraph may, quite wrongly be regarded as proof of great intellect; in the second case the advertiser tries to induce us to believe that smoking X, etc., will bring with it the other benefits. In both cases the argument runs:-

If P, then Q	If he is clever, I will not understand	If you are a handsome athletic male you will smoke X.
Q is true	I do not understand	I intend to smoke X
So P is true	He is clever	I am/will become handsome and athletic

This is similar to the argument used in the natural sciences to 'verify' a theory P. Testing the implications of P is the 'scientific' method (See p.34). But note that we ought to say "P is not disproved" - the argument does not prove P.

Our advertisement does not directly state that smoking X cigarettes gives rise to these or other beneficial consequences - which might be ludicrous or actionable in law - but does seek to set up an association between them in our minds. Much everyday reasoning involves association rather than implication - we argue that A and B tend to happen together or not at all, rather than that A necessarily leads to B, as we do in mathematics. The

"illogicality" may be a consequence of our assigning an 'everyday' meaning to the idea of implication, which is different from its specialised use in logic and in mathematics. We can see the difference by examining the following statements, each of which is logically correct:-

A) *If X* is a Conservative M.P., *he is* entitled to vote in the House of Commons.

B) "If copper is a poor conductor of electricity, then ice floats on water."

Statement A might be objected to because it seems to imply that only Conservative M.P.s are entitled to vote in the House of Commons. (That is not what it says, but it might well be understood in that way). Statement B would be criticised as "wrong" partly because there is no causal connection between its two parts. (It has the form "if P, then Q" where P and Q have nothing to do with each other), but also because P is false, and it is widely accepted that Q ought also to be false in such circumstances. This amounts to saying that, in everyday matters, the implication 'if P then Q' is frequently understood to mean 'P is equivalent to Q' - i.e. 'if P then Q' and 'if Q then P', or in other words that P and Q are true or false together. This usage underlies the popular confusion between theorem and converse,† for it is tantamount to saying 'the converse of a true theorem is also true'. It also explains the false argument discussed earlier, for if the statement 'if P, then Q' is interpreted (wrongly!) to mean $\begin{cases} \text{P true implies Q true} \\ \text{P false implies Q false} \end{cases}$, then the finding 'Q is true' must lead to the conclusion 'P is true'.

In short, implication which is properly regarded as directional, is commonly thought of as symmetric.

We shall examine the logical structure of proofs in more detail in Chapter 5. For the moment we introduce some notation and look at examples of theorem/converse relationships in mathematics.

---

† Demonstrated by a considerable amount of research, some involving highly intelligent adults. See O'Brien, T.C., *Deformation and the Four Card problem*, Educational Studies in Mathematics, 6, 1, Mar. 1975. pp.23-40.

'P implies Q' or 'if P, then Q' is written $P \Rightarrow Q$

The statement which is true when P is false, the negation of P, is written as $\sim P$ (in some texts, $\neg P$). (Thus if P is "Today is Monday", $\sim P$ is "Today is not Monday").

The implication $P \Rightarrow Q$ is understood to mean:-

If P is true then Q must be true.

If P is false then Q may be true or false

This may be expressed in an alternative form as 'either P is false or Q is true (or both)'. (This is written as $\sim P \vee Q$, where '$\vee$' is used for 'or'). Note that it is not necessary for there to be any causal connection between P and Q. (Check that the statements (A) and (B) above satisfy this definition).

The case 'false' $\Rightarrow$ 'true', (rejected in everyday usage), is accepted for two reasons - when we make an assumption in the course of a proof, which may later be proved invalid, (for example, see p. 42) we do not know at that stage whether or not it is true - but must still be left free to investigate its consequences. Further, a false proposition can lead, by strictly logical arguments, to a true conclusion. A simple example is:-

Suppose $3 = 5$

Then $5 = 3$

Adding $8 = 8$ (a true result).

Thus of the following four statements, only one is incorrect. (Which one?).

a) If $2 = 3$ then $7 > 4$

b) If $7 > 4$ then $2 = 3$

c) If $2 \neq 3$ then $7 > 4$

d) If $7 \not> 4$ then $2 = 3$

The converse of the statement $P \Rightarrow Q$ is defined to be $Q \Rightarrow P$. If both the statement and its converse are true, so that $P \Rightarrow Q$ and $Q \Rightarrow P$, we say P and Q are equivalent and write $P \Leftrightarrow Q$. (This means P and Q are either both true or both false).

Exercise 4

4.1 Write the converses of the following five statements. Are the statements true? Are their converses true?

(a) If the product of two numbers is odd, then their sum is even.

(b) If a quadrilateral is a rectangle, then its diagonals are equal in length.

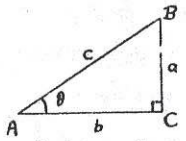
(c) Given two real numbers x, y, if one or both of the numbers is zero, then their product is zero.

(d) Given two 2 x 2 matrices A, B, if one or both of A, B is the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, then $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

(e) If the ΔABC is right-angled at C, then $a^2 + b^2 = c^2$.

4.2 The following are examples of standard mistakes in mathematics. Point out the errors:

(a) To prove (e) above (Pythagoras' theorem)



$a^2 = c^2 \sin^2\theta$, $b^2 = c^2 \cos^2\theta$,

$a^2 + b^2 = c^2(\sin^2\theta + \cos^2\theta) = c^2$, since $\sin^2\theta + \cos^2\theta = 1$.

(b) Theorem: $1 = 2$

Proof: $1 = 2$, $\therefore 2 = 1$, $\therefore 3 = 3$ which is true. $\therefore 1 = 2$

(c) Theorem: any quadratic equation has just two roots.

Proof: Consider $x^2 - 5x + 6 = 0$ or $z^2 + 1 = 0$

These have roots $x = 3, 2$ and $z = j, -j$ respectively

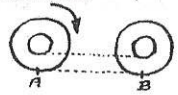
or

Theorem: any four vectors in $\mathbb{R}^3$ are linearly dependent.

Proof: consider (1,0,0) (0,1,0) (0,0,1) and (1,2,3)

(d) Any two circles have equal circumferences.†

Proof:



Both circles roll a distance AB

(e) If A is a 2 x 2 matrix with $A^2 = A$, then either $A = I$ or $A = 0$

(where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\underline{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Proof: If $A = I$, then $I^2 = I$ hence $A^2 = A$

If $A = \underline{0}$, then $\underline{0}^2 = \underline{0}$, hence $A^2 = A$

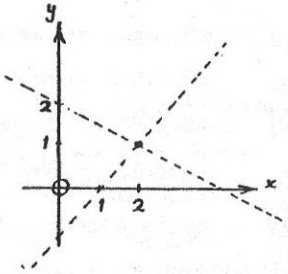
(f) Theorem: $1 + 2 + 4 + 8 + 16 + \ldots = -1$

Proof: Let $1 + 2 + 4 + 8 + \ldots = S$

Then $1 + 2S = S$, $S = -1$

4.3 "The solution of the equations $\left.\begin{matrix} x + 2y = 4 \\ x - y = 1 \end{matrix}\right\}$ is $x = 2$, $y = 1$ "

Which of the following is the best proof? :-



(a) The graphs of the 2 straight lines intersect at the point (2,1)

So $x = 2$, $y = 1$.

(b) Subtracting, $3y = 3$ $y = 1$

From 1st equation, $x = 2$

(c) $x = 2$, $y = 1$ satisfies both equations and so is the solution.

Is your opinion altered if the equations are changed to

$\left.\begin{matrix} 3x + 6y = 6 \\ x - y = 1 \end{matrix}\right\}$ with solution $x = 1\frac{1}{3}$, $y = \frac{1}{3}$?

4.4 (a) If $x = y$ then (α) $3x = 3y$ (β) $x^3 = y^3$ (γ) $x^6 = y^6$

Which of these three deductions is reversible?

(b) Solve $\sqrt{3x + 7} = 2 + \sqrt{x + 3}$

(c) Comment on the following "proof". Given $\frac{p}{q} = \frac{r}{s}$,

to prove $\frac{p^2 + q^2}{r^2 + s^2} = \frac{pq}{rs}$

"Proof" If $(p^2 + q^2)rs = pq(r^2 + s^2)$

then $(pr - qs)(ps - qr) = 0$

so $pr = qs$ or $ps = qr$

But $ps = qr$ is true, so the result is true.

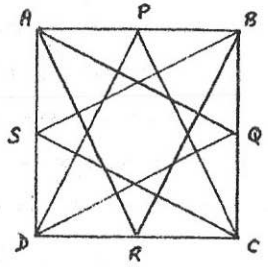
CHAPTER 3

PICTURES: THE POWER AND THE DANGER OF 'VISUAL' PROOFS

In some situations the proof of a statement may be conveyed very vividly by means of a diagram. We have already seen an example (p.4). Such 'proofs' give one a sense of overall comprehension of the theorem which is very valuable - and which is sometimes lost in the detailed process of understanding the formal, step by step, chain of argument which normally constitutes a mathematical proof. It is very useful, in any case, to have a grasp of the 'strategy' of a proof - what the major stages and the crucial steps are, rather than getting lost in the 'tactics' or detail. (This is not to say that detail is unimportant - one flaw *will* render a 'proof' invalid - but that it is easier to understand and remember a proof whose general 'shape' is known).

It is well known that there are dangers in relying on diagrams; some illustrations are given below. Yet it is a mistake to suppose that diagrams are undesirable, or in some way inferior. Many people, including professional mathematicians, find them an indispensible aid to thinking. What is important is to avoid being misled by them. (See pp. 19, 55, also Appendix III A, p 74).

We give first, as a warning, two other examples of fallacies which rely on a visual 'proof'.



(a) ABCD is a square. PQRS are mid-points of sides. AR, BR etc. are drawn, as shown.

Conjecture: "the octagonal region outlined in the centre is regular".

(In fact this is false; the octagon has eight equal sides, but its angles are alternately greater and less than 135^0).

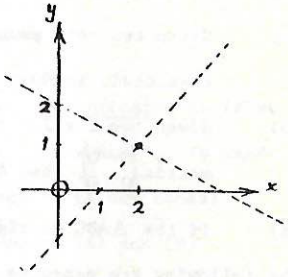
(f) Theorem: $1 + 2 + 4 + 8 + 16 + \ldots = -1$

Proof: Let $1 + 2 + 4 + 8 + \ldots = S$

Then $1 + 2S = S$, $S = -1$

4.3 "The solution of the equations $\left.\begin{matrix} x + 2y = 4 \\ x - y = 1 \end{matrix}\right\}$ is $x = 2$, $y = 1$ "

Which of the following is the best proof? :-



(a) The graphs of the 2 straight lines intersect at the point (2,1)

So $x = 2$, $y = 1$.

(b) Subtracting, $3y = 3$ $y = 1$

From 1st equation, $x = 2$

(c) $x = 2$, $y = 1$ satisfies both equations and so is the solution.

Is your opinion altered if the equations are changed to

$\left.\begin{matrix} 3x + 6y = 6 \\ x - y = 1 \end{matrix}\right\}$ with solution $x = 1\frac{1}{3}$, $y = \frac{1}{3}$?

4.4 (a) If $x = y$ then (α) $3x = 3y$ (β) $x^3 = y^3$ (γ) $x^6 = y^6$

Which of these three deductions is reversible?

(b) Solve $\sqrt{3x + 7} = 2 + \sqrt{x + 3}$

(c) Comment on the following "proof". Given $\frac{p}{q} = \frac{r}{s}$,

to prove $\frac{p^2 + q^2}{r^2 + s^2} = \frac{pq}{rs}$

"Proof" If $(p^2 + q^2)rs = pq(r^2 + s^2)$

then $(pr - qs)(ps - qr) = 0$

so $pr = qs$ or $ps = qr$

But $ps = qr$ is true, so the result is true.

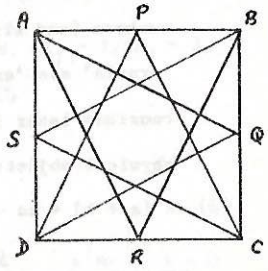
CHAPTER 3

PICTURES: THE POWER AND THE DANGER OF 'VISUAL' PROOFS

In some situations the proof of a statement may be conveyed very vividly by means of a diagram. We have already seen an example (p.4). Such 'proofs' give one a sense of overall comprehension of the theorem which is very valuable - and which is sometimes lost in the detailed process of understanding the formal, step by step, chain of argument which normally constitutes a mathematical proof. It is very useful, in any case, to have a grasp of the 'strategy' of a proof - what the major stages and the crucial steps are, rather than getting lost in the 'tactics' or detail. (This is not to say that detail is unimportant - one flaw *will* render a 'proof' invalid - but that it is easier to understand and remember a proof whose general 'shape' is known).

It is well known that there are dangers in relying on diagrams; some illustrations are given below. Yet it is a mistake to suppose that diagrams are undesirable, or in some way inferior. Many people, including professional mathematicians, find them an indispensible aid to thinking. What is important is to avoid being misled by them. (See pp. 19, 55, also Appendix III A, p 74).

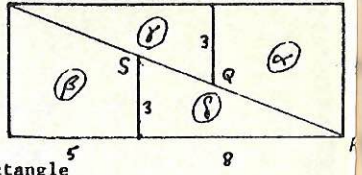
We give first, as a warning, two other examples of fallacies which rely on a visual 'proof'.



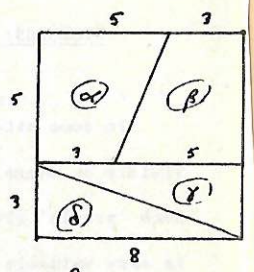
(a) ABCD is a square. PQRS are mid-points of sides. AR, BR etc. are drawn, as shown.

Conjecture: "the octagonal region outlined in the centre is regular".

(In fact this is false; the octagon has eight equal sides, but its angles are alternately greater and less than 135°).

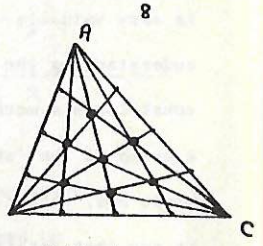


(b) An 8 x 8 square is dissected into four pieces which may be rearranged as shown to form a rectangle 5 x 13. (Yet 5 x 13 = 65 ≠ 64 = 8 x 8).



Exercise 5.1. Cut out the shapes in (b) from thin card and try the rearrangement. Explain the fallacy in (a) and (b).

5.2. Draw any triangle ABC. If A, B, C are joined to the mid points A_1, B_1, C_1 of opposite sides (AA_1 is a median) the 3 lines are concurrent. If the angles at A, B, C are bisected, the 3 bisectors are concurrent.



Investigate the conjectures

(a) If A, B, C are joined to the points of quadrisection of BC etc. the lines are concurrent in threes.

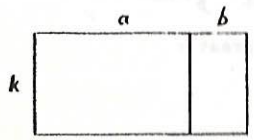
(b) A similar statement about lines which divide the angles into four equal parts.

Some valid demonstrations

(c) 2 x 3 = 3 x 2 o o o / o o o ('Multiplication of natural numbers is commutative')

An array of counters may be seen as '2 lots of 3' or '3 lots of 2'. Evidently a similar display could be produced for any pair of whole numbers (and also for corresponding addition demonstrations). Such 'proofs' are 'experimental', as distinct from the 'axiomatic' ones we consider later (*Appx. I.*), which are independent of the examination of physical objects.

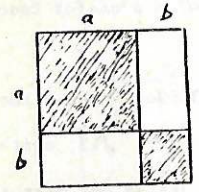
(d) k (a + b) = ka + kb (The distributive law for natural numbers).



Note. The method evidently extends, by a change of measuring unit, to the case where k, a, b are rational numbers (i.e. k = $\frac{\ell}{m}$ etc., ℓ, m natural numbers).

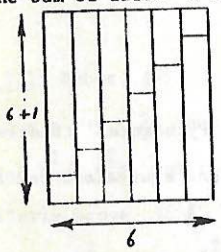
The Greeks were aware that $\sqrt{2}$ is irrational (see p 42), which implies that no unit of measurement exists which is an exact sub-multiple of the lengths 1 and $\sqrt{2}$. They accordingly used this diagram to give a definition of k (a + b), where k, a, b, are now real numbers, and as a proof that k (a + b) = ka + kb for real numbers.

(e)



$(a + b)^2 = a^2 + 2ab + b^2$

(f) The sum of first n natural numbers is $\frac{1}{2}n(n + 1)$



This diagram shows the case n = 6. A similar diagram can be drawn for any n.

Exercise 6.1. Draw similar diagrams for k(a - b), (a + b)(c + d), (a + b)(a - b), $(a - b)^2$ (areas overlapping), and $(a + b)^3$ (volumes), and $a^3 + b^3$ (harder).

6.2. Draw diagrams to illustrate

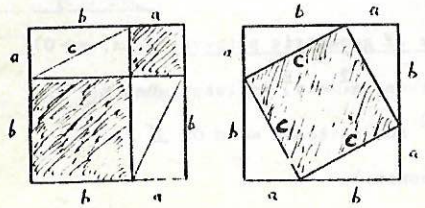
$1 + 3 + 5 + 7 = 4^2$

$1 + 2 + 3 + 4 + 3 + 2 + 1 = 4^2$

$T_3 + T_4 = 4^2$ where T_n is the nth triangular number. $T_1 = 1$, $T_2 = 3$, $T_3 = 6$, $T_4 = 10$, etc.

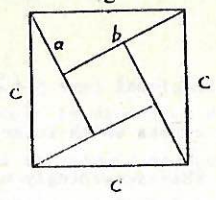
(g) Pythagoras' theorem

(i)



$a^2 + b^2 + 4\Delta$

$= c^2 + 4\Delta$

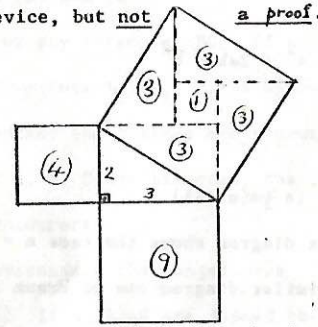
(ii) 

$c^2 = 4(\frac{1}{2}ab) + (b - a)^2$

$= 2ab + (b - a)^2$

$= \underline{a^2 + b^2}$

This method involves algebraic manipulation; in any particular numerical case, this gives a simple *demonstration* allowing pupils to arrive at Pythagoras' theorem "by observation" - a useful teaching device, but not a proof.

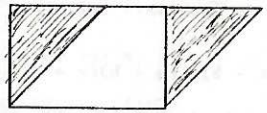


e.g. a = 2, b = 3 (Note that although $c = \sqrt{13}$, neither surds nor measurement are involved).

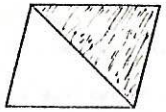
4 + 9 = 13

(See Appendix IIIA for further discussion of Pythagoras' theorem).

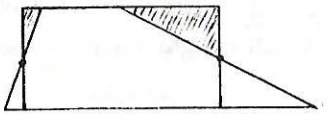
(h) (i) Parallelogram and equivalent rectangle.

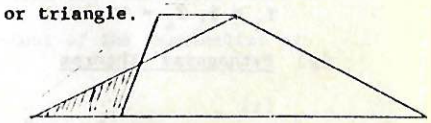


(ii) Triangle as half parallelogram.



(iii) Trapezium and equivalent rectangle or triangle.

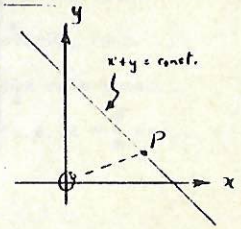




(j) Inequalities by use of geometric properties (x, y > 0)

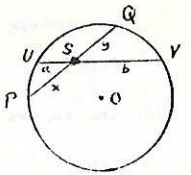
(1) If x + y is given, $x^2 + y^2$ is least when x = y:-

($x^2 + y^2 = OP^2$ and is least when OP ⊥ line x + y = const.).

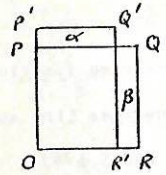


(2) If xy is given, x + y is least for x = y:-

Let xy = ab; then x + y is represented by the chord PQ of the circle†, and PQ is least when the perpendicular from O to PQ is greatest - i.e. when it falls at S.



(3) If x + y is given, xy is greatest when x = y.



Let OPQR be a square, side a.

Let P'Q' = x = a - e.

Q'R' = y = a + e. (PP' = e = R'R).

Area PQRO - Area P'Q'R'O = $\beta - \alpha > 0$ since each rectangle has width e, and QR = a > P'Q'.

Exercise 7.1. Prove j(2) implies j(3). (Use an argument by contradiction:-

Suppose x + y = 2d, but that the greatest value of xy is f^2, (where $f^2 > d^2$), and that it occurs when $x \neq y$).

7.2. Similarly prove j(3) implies j(2).

7.3. Use $(x + y)^2 + (x - y)^2 \equiv 2(x^2 + y^2)$ and $(x + y)^2 - (x - y)^2 \equiv 4xy$ to prove all of (j).

7.4. (An extension of j(3)). If three numbers x, y, z, all positive, have a given sum, their product is greatest when all are equal.

(Hint : use an algebraic method. Regard z as, temporarily, fixed).

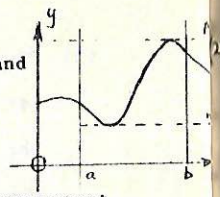
7.5. Adapt j(1) to find the minimum of $x^2 + y^2$ given that 2x + y is fixed.

(For an extensive treatment of inequalities based on this approach see Fletcher, T.J., Math. Gazette 391, Feb. 1971 pp.4-17).

---

† We use the "rectangle property" of a circle — US.SV = PS.SQ.

(k) (1) If the function f(x) may be integrated for $a \leq x \leq b$ and has greatest and least values M and m in this interval, then $m(b-a) \leq \int_a^b f(x)dx \leq M(b-a)$.

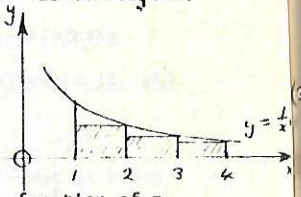


(2) The series $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots = \sum_1^\infty \frac{1}{r^2}$ is convergent.

Proof:

$$\frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2} = \sum_2^n \frac{1}{r^2} < \int_1^n \frac{1}{x^2}dx$$

$$= \left[-\frac{1}{x}\right]_1^n = 1 - \frac{1}{n}$$

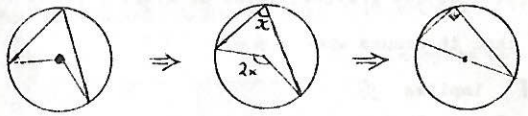


Thus the sum to n terms, which is an increasing function of n, is bounded above by 2, and the series converges (its sum is $\frac{\pi^2}{6}$, see p.48). (See also Appendix IIIA, 4 and 5, p74).

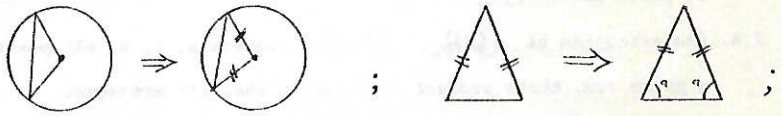
(l) Diagrams may be useful in indicating the structure of a proof, as is page-layout.

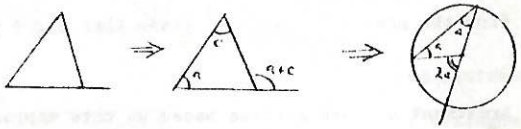
Examples:

(1) [Skemp, 1971, p 106, adapted] †

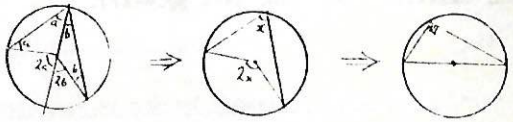


Proof

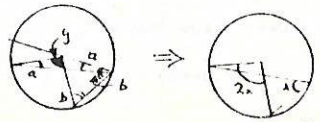




Case (i)



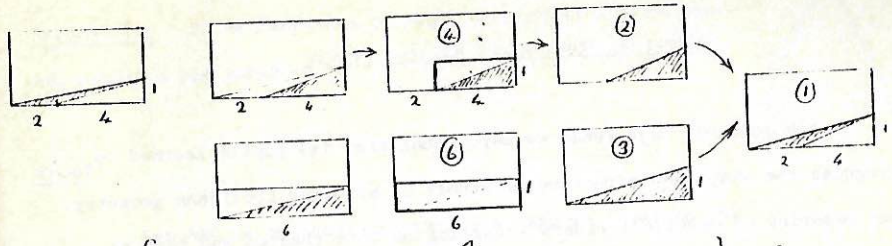
Case (ii)



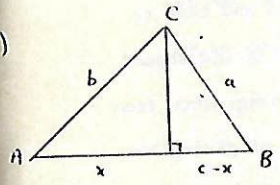
$y = 2b - 2a = 2(b-a)$

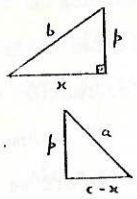
† Reprinted by permission of Penguin Books Ltd

(2)



(3)





$x^2 = \ldots\ldots$

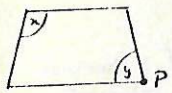
$(c-x)^2 = \ldots\ldots$

$c^2 = \ldots\ldots$

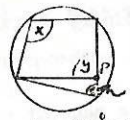
$a^2 = \ldots\ldots$

(Cosine rule).

(4)

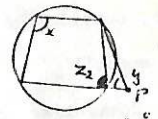


To prove. $x + y = 180^\circ \Rightarrow$ cyclic.



$x + z_1 = 180^\circ \Rightarrow y = z_1$

But $y > z_1$.



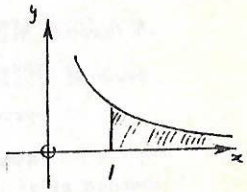
$x + z_2 = 180^\circ \Rightarrow y = z_2$

But $y < z_2$

Hence P must lie on circle.

(m) A final reminder of the dangers inherent in 'pictures and commonsense':-

Consider the region (shown shaded) between the x-axis and the curve $y = \frac{1}{x}$ for $x > 1$. The area of this region is $A = \int_1^\infty \frac{dx}{x}$, and the volume V obtained by rotating it about the x-axis is $\int_1^\infty \frac{\pi}{x^2}dx = \pi$



But the integral A does not exist (is infinite) - so we have the 'paradoxical' result that the volume of paint which could be contained in V is π units, yet an infinite amount of paint would be needed to paint the area A.†

† We tend to think of the paint as applied with uniform thickness - but the dimensions of the trumpet shape V tend to zero as $x \to \infty$.

CHAPTER 4

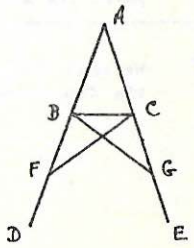
Advice on Reading and Writing Proofs

In the good old days (when we were young that is) pupils learned to recognise the shape and structure of proofs by studying Euclidean geometry. What memories of countless riders - calling on this theorem and that to follow angles and sides around complicated scaffolds built in and around several circles; assembling enough information to follow congruence from triangle to overlaid triangle. No wonder we are in danger of giving the impression that a 'proof' is something as old as time, pure and untouchable, outside the reach of ordinary mortals - so superior to a mere 'ar-ument'!

Commenting on Dr. Watson's account of one of his cases (†) Sherlock Holmes tells him

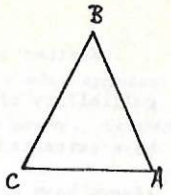
> 'Honestly, I cannot congratulate you upon it. Detection is, or ought to be, an exact science, and should be treated in the same cold and unemotional manner. You have attempted to tinge it with romanticism, which produces much the same effect as if you worked a love-story or an elopement into the fifth proposition of Euclid!'

No doubt Euclid himself would have agreed - one tends to regard one's own proofs with special reverence! The account of the fifth proposition in the Elements begins with this heartsinking diagram and continues for forty seven lines; eight triangles to boggle the mind.



It seems likely however that Pappus, writing seven hundred years later, would take a warmer more human view. His proof of the same proposition is a delight (Heath, (1926), Vol I, p.254).

† The Sign of Four . Sir A. Conan Doyle.



Proposition In an isosceles triangle the angles at the base are equal to one another.

Proof

Let ABC be an isosceles triangle, and AB equal to CB.

Let us conceive this one triangle as two triangles.

$AB = CB$ given,

$BC = BA$ given,

$\hat{ABC} = \hat{CBA}$ common.

Therefore triangles ABC and CBA are congruent (Proposition 4).

Hence $\hat{CAB} = \hat{ACB}$ (corresponding angles).

The point is that proofs differ in quality. They are valued, believe it or not, largely on the basis of their clarity and their simplicity. The object of the proof is to bridge the gap from hypothesis to conclusion in as obvious a way as possible. In the case of Proposition 5 the essential feature is the symmetry of the isosceles triangle about the median through B. Pappus' proof is simpler, clearer and therefore better than Euclid's because it is closer to this basic property.

We are not stuck with a proof in the precise form in which it is handed down to us. If we feel that we dare not alter a word then we certainly have not understood it. Far from 'parrot learning' the understanding of a proof leads to the freedom to rephrase it, reshape it and split it up in a way which makes it more understandable and more suggestive of what is going on underneath.

The development of any part of mathematics, perhaps over hundreds of years, is essentially a process of finding a way of approaching complicated awkward situations through a sequence of obvious commonsensical steps. From this point of view the sacred untouchable 'proof' becomes merely a convincing argument - the simpler the better.

Whether a proof is convincing or not might seem to depend upon the gullibility of the reader! In order to guard against being duped we have extracted rules of sound argument (see chapter 6) which we must always have at the front of our minds when reading mathematics. The examples in chapter 2 show the dangers of forgetting them.

Let us assume that you are interested in a particular theorem or conjecture and that you have the ingredients of what you believe will be a convincing argument. The next stage is to find a way of communicating that argument to a reader.

Always remember to make the argument as simple and clear as possible. Do not try to impress him with the difficulty of it all. It may be galling but you must leave on one side all the impossible tangles which you got into. You are allowed a wry smile when the reader says 'well that seems straight forward' but no more. Who knows how long Pappus laboured before he found the key line 'Let us conceive this one triangle as two triangles'?

Test your style by reading the proof aloud - with symbols translated. It should read like a piece of prose - it must do otherwise there is no argument there. Do not just slap down a collection of equations leaving the reader to invent the connections. The subject is difficult enough as it is without making a jig-saw of it.

Here is a result about geometric and arithmetic means.

Theorem. Let a and b be positive numbers. Then $\frac{1}{2}(a+b) \geq (ab)^{\frac{1}{2}}$.

'Proof'.
$$\frac{1}{2}(a+b) \geq (ab)^{\frac{1}{2}}$$
$$(a+b)^2 \geq 4ab$$
$$a^2+b^2-2ab \geq 0$$
$$a^2+b^2-2ab = (a-b)^2 \geq 0$$
$$\therefore \frac{1}{2}(a+b) \geq (ab)^{\frac{1}{2}}$$

This really doesn't make sense and even to the most indulgent reader appears to make the standard mistake of assuming what we are trying to prove. Compare

Proof We want to show that $\frac{1}{2}(a+b) \geq (ab)^{\frac{1}{2}}$.

Since a and b are positive this will follow if

$$(a+b)^2 \geq 4ab.$$

This in turn will follow if

$$a^2+b^2-2ab \geq 0.$$

But for all a and b

$$a^2+b^2-2ab = (a-b)^2 \geq 0.$$

$$\therefore \frac{1}{2}(a+b) \geq (ab)^{\frac{1}{2}}.$$

The equations are just the same - the words between make all the difference. No doubt they were in the mind of the writer of the first 'proof' but the reader needs to be told what they are.

Help the reader to find his way through the argument. Some proofs involve just starting with the hypothesis and then following your nose until you get to the conclusion. Others adopt one of the less direct approaches described in later chapters. In this case it is helpful to the reader to declare at the beginning what strategy you are going to adopt - 'This theorem will be proved by contradiction', 'We will prove this theorem by induction' or whatever.

Many proofs rest on just one or two key ideas (Pappus' second line for example), with fairly obvious steps in between. Make sure that the reader has every chance of seeing those ideas as the scaffolding around which the proof is built.

Choose your notation carefully. The development of mathematics is very much bound up with finding economical managable notations. It is no wonder that the Romans contributed nothing to the subject and that the Babylonians contributed so much. If possible choose a notation which will help the reader - don't use ϵ for a large negative number, don't use a and b for variables and so on.

Many longer proofs divide up into sections - try to keep them clear of each other with signposts and labels. It might be worth taking a subsection out altogether and establishing it as a Lemma in preparation for a proof of the main theorem. Do everything you can to lay out what is going on as clearly as possible.

Here is an example:-

Theorem (Gaston Darboux 1842-1917)	Human interest,
Let $f: \mathbb{R} \to \mathbb{R}$ be a differentiable function and let $f'(a) < \gamma < f'(b)$ where $a < b$.	Hypothesis,
Then there exists $c \in]a,b[$ such that $f'(c) = \gamma$.	Conclusion,
Proof Define a function $g: [a,b] \to \mathbb{R}$ by the rule $g(x) = f(x) - \gamma x$, $x \in [a,b]$.	A new idea - slightly mysterious at this stage.
The function g is differentiable and $g'(x) = f'(x) - \gamma$, $x \in [a,b]$.	Not so mysterious now.
We will show that the infimum of g does not occur at a or at b.	Plan - the key idea.
It will follow that the infimum is attained at some c with $a<c<b$.	Use of a previous theorem
Hence $g'(c) = 0$ and so $f'(c) = \gamma$.	Use of a previous theorem
Now $g'(a) = f'(a) - \gamma < 0$ $\therefore$ $g(a+h) < g(a)$ for small $h>0$. Similarly $g'(b) = f'(b) - \gamma > 0$ $\therefore$ $g(b-k) < g(b)$ for small $k>0$.	Technical section. Perhaps worth treating as a Lemma.
Hence g does not attain its infimum either at a or b.	The point of technical section
It therefore attains the infimum at some point between a and b. At such a point $g'(c) = 0$. Therefore $f'(c) = \gamma$	One triumph after another

You will find another example of such an analysis at the end of Appendix IV.

After you think you have finished - think again. Have you proved the theorem or its converse? Are there special cases which you have not allowed for. Would it be possible to simplify the argument - perhaps by proving preliminary theorems or lemmas?

'Theorem' For all real numbers a, b and c if $ac = bc$ then $a = b$.

'Proof' If $ac \neq bc$ then $c \neq 0$; hence $a \neq b$.

or

'Proof' If $ac = bc$ then $(ac)\frac{1}{c} = (bc)\frac{1}{c}$.

Hence $a = b$.

The converse of the 'theorem' is true but the 'theorem' itself is false ($1 \times 0 = 2 \times 0$). (It becomes true, of course, if we exclude the possibility of c being 0). There is no need to be polite about it - mark it wrong! We mustn't turn a blind eye to the one blemish among the infinity of correct cases covered.

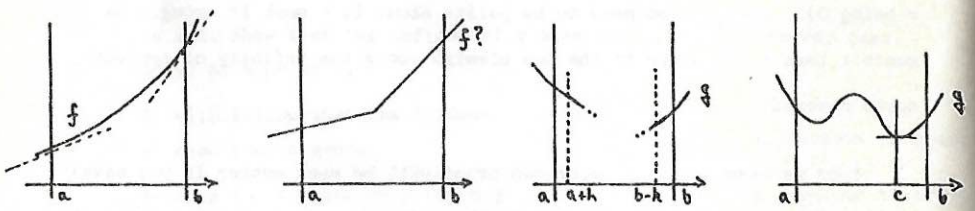
Your re-examination of your own proof will be much easier if you have taken steps to help the reader to see the structure. Most crank efforts at achieving the impossible (squaring the circle and so on, p.87) have their flaw in the middle of a hopeless muddle.

Your own experience of constructing proofs will help you to read other peoples efforts. Understanding a theorem and its proof can take a long time, there is no shame in taking it very slowly. Look at the statement of the theorem first of all. Make sure that you are thoroughly familiar with the words used and the notation. Draw pictures and try examples to test the theorem out. In this way you will become almost certain that the theorem is true. The purpose of the proof is firstly to lift 'almost certain' into 'certain' and secondly to explain why the theorem must be true.

In reading other people's proofs remember the difficulty you have in writing your own. Arguments which seem clear and simple in one's head can turn out messy and complicated on paper. Do not expect to read through a proof line by line and obtain the complete understanding which you do from reading a light novel. Quite often one has to identify the main strategy first, then some major points in the proof and finally understand the technical details which fill in the spaces.

Try to split the proof up into sections as we have done with the above proof of Darboux' theorem (a super theorem really - it makes it easy to invent functions which are not the derivatives of anything). If you can see the overall strategy and the shape you are well on the way to understanding the argument. The small technical details, use of other theorems etc. are then isolated and can be picked off one at a time.

Draw lots of pictures if at all possible to illustrate what is going on. Here are some related to Darboux' theorem.



Apply the theorem in special cases. What can go wrong if individual items in the hypothesis are altered? Such exploration will give you a feel of the theorem and the given proof. It is <u>not</u> enough just to follow the argument through from one line to the next. Full understanding comes from an awareness of the proof as a whole. It is at that stage that you will want to put the book away and write to the author tactfully explaining how much more clearly his proof could have been expressed!

CHAPTER 5

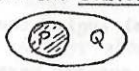
<u>LANGUAGE AND NOTATION</u>. <u>STRATEGIES OF PROOF</u>

<u>The use of logical notation in discussing proof structure</u>

A conditional statement can be represented by $P \Rightarrow Q$ or 'If P, then Q'. or 'P implies Q' where P represents the hypothesis and Q represents the conclusion. As an example,

let P represent the statement 'I am eating',

let Q represent the statement 'I am awake'.

Then $P \Rightarrow Q$ is (for normal people!) a true implication. The statement $Q \Rightarrow P$ ('If I am awake, I am eating') does <u>not</u> mean the same thing and is <u>not</u> true (of most people!). (It is the <u>converse</u> statement.) We can also use a diagram to illustrate:- 

The set of possibilities in which P is true is entirely included in that for which Q is true. So, "if P is true, Q follows". $P \Rightarrow Q$.

Note that the diagram also represents "If *not* Q *then* not P", which may be written $\sim Q \Rightarrow \sim P$. This form of the statement $P \Rightarrow Q$ is called the <u>contrapositive</u> (i.e. $\sim Q \Rightarrow \sim P$.) - note that the roles of P and Q are interchanged <u>and the two negation signs are *attached*</u>. This statement says <u>exactly the same</u> as $P \Rightarrow Q$ (i.e. the statements are equivalent: think about it!) If the roles of P and Q are interchanged <u>without</u> introducing negation symbols, we obtain the <u>converse</u> $Q \Rightarrow P$. This is <u>not</u> equivalent to $P \Rightarrow Q$ (see Chapter 2).

An example may help:

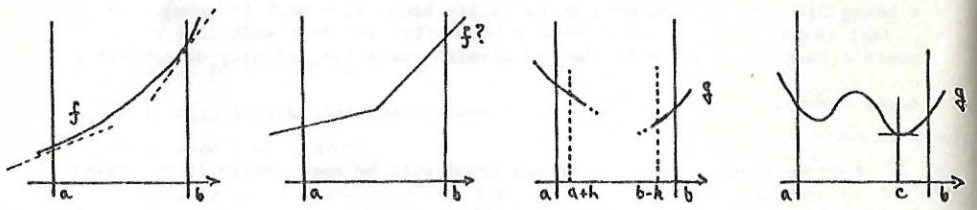
P This animal is a dog

Q It has four legs

In reading other people's proofs remember the difficulty you have in writing your own. Arguments which seem clear and simple in one's head can turn out messy and complicated on paper. Do not expect to read through a proof line by line and obtain the complete understanding which you do from reading a light novel. Quite often one has to identify the main strategy first, then some major points in the proof and finally understand the technical details which fill in the spaces.

Try to split the proof up into sections as we have done with the above proof of Darboux' theorem (a super theorem really - it makes it easy to invent functions which are not the derivatives of anything). If you can see the overall strategy and the shape you are well on the way to understanding the argument. The small technical details, use of other theorems etc. are then isolated and can be picked off one at a time.

Draw lots of pictures if at all possible to illustrate what is going on. Here are some related to Darboux' theorem.



Apply the theorem in special cases. What can go wrong if individual items in the hypothesis are altered? Such exploration will give you a feel of the theorem and the given proof. It is <u>not</u> enough just to follow the argument through from one line to the next. Full understanding comes from an awareness of the proof as a whole. It is at that stage that you will want to put the book away and write to the author tactfully explaining how much more clearly his proof could have been expressed!

CHAPTER 5

LANGUAGE AND NOTATION. STRATEGIES OF PROOF

The use of logical notation in discussing proof structure

A conditional statement can be represented by $P \Rightarrow Q$ or 'If P, then Q'. or 'P implies Q' where P represents the hypothesis and Q represents the conclusion. As an example,

let P represent the statement 'I am eating',

let Q represent the statement 'I am awake'.

Then $P \Rightarrow Q$ is (for normal people!) a true implication. The statement $Q \Rightarrow P$ ('If I am awake, I am eating') does <u>not</u> mean the same thing and is <u>not</u> true (of most people!). (It is the <u>converse</u> statement.) We can also use a diagram to illustrate:-

The set of possibilities in which P is true is entirely included in that for which Q is true. So, "if P is true, Q follows". $P \Rightarrow Q$.

Note that the diagram also represents "If *not* Q *then* not P", which may be written $\sim Q \Rightarrow \sim P$. This form of the statement $P \Rightarrow Q$ is called the <u>contrapositive</u> (i.e. $\sim Q \Rightarrow \sim P$.) - note that the roles of P and Q are interchanged <u>and the two negation signs are *attached*</u>. This statement says <u>exactly the same</u> as $P \Rightarrow Q$ (i.e. the statements are equivalent: think about it!) If the roles of P and Q are interchanged <u>without</u> introducing negation symbols, we obtain the <u>converse</u> $Q \Rightarrow P$. This is <u>not</u> equivalent to $P \Rightarrow Q$ (see Chapter 2).

An example may help:

P This animal is a dog

Q It has four legs

Statement	Converse	
$P \Rightarrow Q$ (T)	$Q \Rightarrow P$ (F)	Note the converse is <u>false</u> ("miaow"!)
$\sim P \Rightarrow \sim Q$ (F)	$\sim Q \Rightarrow \sim P$ (T)	The contrapositive is <u>true</u>
Inverse	Contrapositive	

The form $\sim P \Rightarrow \sim Q$ is called the <u>inverse</u>. It is true whenever the converse is true. (In fact it is the contrapositive form of the inverse (!)).

In sum:-

Statement and contrapositive : True or false together

Converse and inverse : True or false together

<u>But</u>, statement and converse are logically independent of each other.

<u>Note</u>. In the subject of mathematical logic, the algebra of statements is studied using the notation; our concern here is solely to make use of this symbolism to clarify our discussion of proof methods and of errors in logical argument.

<u>Logically equivalent statements</u>. $P \Leftrightarrow Q$

If two statements are always true or false <u>together</u>, they are logically equivalent. 'If P, then Q' and 'If Q, then P' are both true in this case. The statement '$P \Rightarrow Q$ <u>and</u> $Q \Rightarrow P$' can be written as '$P \Leftrightarrow Q$'.

<u>Example</u> considering a quadrilateral S

P_1: 'S has both pairs of opposite sides parallel'

Q_1: 'S has both pairs of opposite sides equal.'

Then $P_1 \Leftrightarrow Q_1$.

A <u>definition</u> is a special form of equivalence in which a name or classification is assigned to an object. e.g. suppose we denote the definition by D.

D: 'S is a <u>parallelogram</u>'

then $P_1 \Leftrightarrow D$. This illustrates the two aspects of a <u>definition</u> - every object which satisfies the condition P receives the label 'parallelogram' and conversely, every object given the label must satisfy the condition P.

The obvious way of checking whether an object belongs to a particular class is to examine whether it satisfies the definition for that class. e.g. to show that the set $\{1, -1, j, -j\}$ is a group under multiplication, we have to verify that the four group axioms (of Closure, Associativity, Identity and Inverse) are satisfied. $(j^2 = -1)$.

A synonym for "$\Leftrightarrow$" is "iff", if-and-only-if

'S is a parallelogram if and only if both pairs of opposite sides are parallel.'

<u>Note</u> on "if", "only if," "necessary", and "sufficient". These may cause confusion and the use of symbols is often helpful.

<u>Example</u>. Suppose a University writes to an A-level candidate. "You will be admitted to the Dept. of Egyptology if you obtain 3 "B's" at A-level."

We may write P : Obtain 3 B's at A-level

Q : Admitted to Dept. of Egyptology.

Then this statement means $P \Rightarrow Q$. Note that nothing is said about what happens if he fails to get 3 B's - he <u>may</u> still be admitted (3 B's are a sufficient - but not necessary - condition for entry).

Suppose, however, the offer states

"You will be admitted to the Dept. of Egyptology only if you obtain 3 B's at A level."

The meaning is now $Q \Rightarrow P$, and he <u>may</u> not be admitted <u>even if</u> he has 3 B's. 3 B's are now a <u>necessary</u> (but not sufficient) condition for entry.

Again the contrast with everyday usage is apparent.

Exercise 8

8.1 Given the statement "If it is sunny, I will go bathing", which of the following is logically equivalent to it. (You may find it helpful to write the statement as S $\Rightarrow$ B)

1. A necessary condition for me to go bathing is that it is sunny.
2. I will go bathing only if it is sunny.
3. It will be sunny only if I go bathing.
4. A necessary condition for it to be sunny is that I go bathing.
5. A sufficient condition for me to go bathing is that it is sunny.
6. If it isn't sunny then I won't go bathing.
7. If I don't go bathing then it isn't sunny.

8.2 Establish necessary and sufficient conditions, in terms of A, B and C, that $Ax^2 + Bx + C > 0$ for all real values of x.

8.3 Replace the dash in each of the following statements by one of the following: N and S, N but not S, S but not N, neither N nor S:-

1. A - condition that x = y is $x^2 = y^2$
2. A - condition that a number is a multiple of 4 is that the number formed by its last two digits is a multiple of 4.
3. A - condition that xy = 0 is that x = 0 and y = 0.
4. A - condition that all the sides of a triangle are equal is that all the angles are equal.
5. A - condition that all the sides of a quadrilateral are equal is that all the angles are equal.
6. A - condition that Peter and Paul are brothers is that they have a common grandfather.
7. A - condition that the sum of two numbers is odd is that their product is even.

Examples of some proof strategies

(a) Note A definition involves a two-way implication - i.e. an equivalence. Thus a statement such as "If 2 triangles are congruent their corresponding angles are equal" is not a definition; it says only C $\Rightarrow$ A, and the statement A $\Rightarrow$ C is false.

(i) In three dimensions, two planes are parallel iff they do not intersect. $\sim I \Leftrightarrow P$ This is a valid definition.

(ii) A rectangle is an equiangular quadrilateral. $\begin{matrix} R \Rightarrow E \\ E \Rightarrow R \end{matrix}$

(b) Proving necessary and sufficient conditions may involve

	(P $\Rightarrow$ Q) and (Q $\Rightarrow$ P)	proposition and converse
or	(P $\Rightarrow$ Q) and ($\sim$P $\Rightarrow$ $\sim$Q)	proposition and inverse
or	P $\Leftrightarrow$ Q $\Leftrightarrow$ R $\Leftrightarrow$ S	i.e. P iff S using the transitivity of implication.

(Note: a necessary and sufficient condition is not unique; in the last case P, Q, R are all necessary and sufficient conditions for S.)

(c) For a series $\sum_1^\infty u_n$ to be convergent it is necessary that $u_n \to 0$ as $n \to \infty$. (See (g) below). However this is not sufficient, since $\sum_1^\infty \frac{1}{n}$ is divergent (See (h) below). Thus (Cgt) $\Rightarrow$ ($u_n \to 0$) but not conversely.

(d) x is even $\Leftrightarrow$ x^2 is even.

(i) $x = 2k \Rightarrow x^2 = 4k^2$ which is even

(ii) x^2 even $\Rightarrow$ x has factor 2 by Unique Factorisation theorem.

Hence, conversely, (or Suppose x is not even, x = 2k + 1; then $x^2 = 4k(k + 1) + 1$ which is not even. Hence by inverse).

(e) Most proofs involve a simple deductive chain of the type

P $\Rightarrow$ Q, Q $\Rightarrow$ R, R $\Rightarrow$ S, from which we conclude P $\Rightarrow$ S, by the rules of 'informal' logic. (The statement $\left.\begin{matrix} P \Rightarrow Q \\ Q \Rightarrow R \end{matrix}\right\} \Rightarrow (P \Rightarrow R)$

is a "theorem" of mathematical logic (see p. 102 and p 69).)

Where the route from hypothesis to conclusion unfolds naturally, constructing it is a matter of "following one's nose".

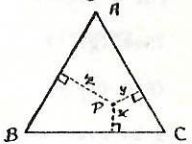
As an example we may prove:-

"The set $\{1, -1, j, -j\}$, where $j^2 = -1$, forms a group under the operation of multiplication." (We have only to check that the four 'group postulates' are obeyed - i.e. that the set is closed under multiplication, that multiplication is associative, that the set contains an identity element (viz. 1), and that each element has a multiplicative inverse in the set. $(1 \times 1 = -1 \times -1 = j \times -j = 1)$

(f) Sometimes - (often!) - a proof depends on looking at the situation in a particular way. ("It ought to be easy to prove this result. What we need is a good idea"). This example, and the next two, provide illustrations.

'P is a point inside an equilateral triangle of side 2a. The perpendiculars from P to the sides of the triangle have lengths x, y, z. Show that $(x + y + z)$ is constant for all positions of P inside the triangle.

This follows easily from a consideration of areas:-



(g) $\sum_1^\infty u_n$ convergent $\Rightarrow$ $u_n \to 0$ as $n \to \infty$:-

Proof: Write $S_n = \sum_1^n u_r$; then $\sum_1^\infty u_n$ convergent $\Rightarrow S_n \to S$ as $n \to \infty$.

Hence $S_{n-1} \to S$ as $n \to \infty$. Thus $u_n = (S_n - S_{n-1}) \to S - S = 0$

(h) $\sum_1^\infty \frac{1}{n}$ is not convergent :-

$S_8 = 1 + \frac{1}{2} + (\frac{1}{3} + \frac{1}{4}) + (\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}) > 1 + \frac{1}{2} + (\frac{1}{4} + \frac{1}{4}) + (\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8})$

Similarly $S_{2^k} > 1 + \underbrace{\frac{1}{2} + \frac{1}{2} + \frac{1}{2} \ldots + \frac{1}{2}}_{k \text{ terms}} = 1 + \frac{k}{2}$

$S_{2^k} \to \infty$ as $k \to \infty$, and so $S_n \not\to S$ as $n \to \infty$ i.e. divergent

(i) Proof by exhaustion.

(1) There is no solution of $x^2 \equiv 2 \pmod 5$:-

For $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9 \equiv 4$, $4^2 \equiv 16 \equiv 1$, $0^2 \equiv 0$,

and there are no other possibilities.

(2) The binary operation on $\{a, b, c, d\}$ defined by the table is commutative.

Each of the possible cases must be checked.

1st \ 2nd	a	b	c	d
a	a	c	d	b
b	c	b	a	d
c	d	a	c	a
d	b	d	a	d

$a * b = c = b * a$

$a * c = d = c * a$

$a * d = b = d * a$

$b * c = a = c * b$

$b * d = d = d * b$

$c * d = a = d * c$

Since there are no other possibilities, the operation is commutative.

(3) There is no solution in integers of $x^2 + y^2 = 11$

Proof: Let $x = 1$; if $y = 1$, $x^2 + y^2 = 2$

$y = 2$, $x^2 + y^2 = 5$

$y = 3$, $x^2 + y^2 = 10$

$y = 4$, $x^2 + y^2 > 11$

Let $x = 2$; if $y = 1$, $x^2 + y^2 = 5$

$y = 2$, $x^2 + y^2 = 8$

$y = 3$, $x^2 + y^2 > 11$

Let $x = 3$; if $y = 1$, $x^2 + y^2 = 10$

$y = 2$, $x^2 + y^2 > 11$

Let $x = 4$; then $x^2 + y^2 > 11$

Thus we have exhausted all possibilities. (Negative values may be ignored).

(Note: We could have reduced the labour of checking by using symmetry, and considering only solutions in which $y \geq x$).

Proof by Mathematical Induction

Induction in the sciences

Scientists and engineers carry out experimental investigations, collect and analyse data, form conclusions and sometimes make predictions which may be tested by further experiments. Even so, they can never be sure that their predictions are correct, for they are based upon induction, the process of inferring general laws from observations of particular instances, and upon analogy, reasoning from apparently similar cases. Neither process provides proof. No matter how many experiments are made, the scientist cannot prove that Newton's law of gravitation will apply in all circumstances. We cannot be sure that the picture of the physical world which we have is a complete one, or that the world itself is not changing; all we can do is assume that our current theories, the best explanations we can give, will continue to be useful in the future.

We have seen already that the checking of particular cases, no matter how many cases are considered, is not sufficient to produce a mathematically acceptable proof, (except in those situations when the number of possible cases is finite - see page 32).† In mathematics the proof of a theorem involves a process of deductive reasoning from certain initial assumptions (sometimes stated explicitly and called 'axioms' or 'postulates', see page 53), with the property that if someone agrees to accept the initial assumptions, he is then forced to accept also the theorem, as one of the conclusions to which they logically lead. (In some areas of science a similar theoretical superstructure, based upon agreed assumptions, has been constructed - for example, the deductions which may be made in mechanics as consequences of Newton's three laws of motion and his law of gravitation.) The role of the inductive method in mathematics, as a way of discovering initial conjectures or proofs is considered later. (page 47 ff.).

(†) Bell (1952), p228, gives an amusing account of Cole's proof to the American Mathematical Society that $2^{67} - 1$ is composite. (Also see p.96).

Mathematical induction is in some ways misnamed, being accepted by mathematicians as a rigorous form of deductive reasoning. It is used when the theorem is a statement about all natural numbers. For example, for all natural numbers n we have:-

$$1 + 2 + 3 + \ldots + n = \frac{n(n + 1)}{2}.$$

(compare p.15). In essence it consists of a way of demonstrating that the proof mechanism is independent of any particular number involved in it, by showing that if the result is true for some particular number k, it will also be true for the next number k + 1. We then, in a typical case, show that the result is true for the number 1, so that it will be true for 2, for 3, for 4, ... and so on. (Just as when the first of a row of dominoes standing on end close together is knocked over, it will knock over its neighbour and the disturbance will be transmitted along the whole row.) We may write P_k to mean "the proposition *when n takes the value k*". The domino analogy reminds us of two matters:-

The first domino must be knocked over; (that is, we must prove P_1 *is true*) and then *the* disturbance must be transmitted along the row, that is, we must prove that $P_k \Rightarrow P_{k+1}$ *is true*.

Another analogy may also be helpful - a sergeant major, wishing to pass on a message to his men assembled in a row on parade, may either announce it to everyone at once (this corresponds to the general direct proof) or (i) instruct each man to pass on (*accurately!*) any message received from one neighbour to his other neighbour, and (ii) tell one man at the end of the row (this corresponds to the two aspects of a proof by mathematical induction).

It is particularly useful in checking conjectures, and indeed depends on knowing the result one wishes to prove. Regarded by some as "the method in which you assume what you have to prove, and then prove it", it is often

misunderstood, and so we shall consider in detail how it is used to prove that $1 + 2 + 3 \ldots + n = \frac{n(n+1)}{2}$

Suppose we have checked that $1 + 2 + 3 \ldots + 12 = \frac{12.13}{2}$

Then $1 + 2 + 3 \ldots + 12 + 13 = \frac{12.13}{2} + 13 = 13(\frac{12}{2} + 1) = 13.\frac{14}{2}$

We started from the truth of the proposition when n = 12, i.e. from P_{12}. Now we are convinced it is true for n = 13; that is we have shown $P_{12} \Rightarrow P_{13}$. The essence of the proof if that it does not depend on particular properties of the number 12. Any number would do instead of 12 - and if we replace 12 by k, we have:-

Assume $1 + 2 + 3 \ldots + k = \frac{k(k+1)}{2}$ (* see below)

Then $1 + 2 + 3 \ldots + k + (k + 1) = \frac{k(k+1)}{2} + (k + 1) =$

$(k + 1)(\frac{k}{2} + 1) = \frac{(k+1)(k+2)}{2}$

This is of the same form but with k replaced by k + 1. Some confusion may arise since we haven't said what k is - it looks like a variable and so why should we not just write (k + 1) instead of k? (When we say $x^2 - 1 \equiv (x + 1)(x - 1)$ for all x, we can write $4y^2 - 1 = (2y + 1)(2y - 1)$ by substituting 2y for x). But when we make the assumption - at the stage marked (*) above - k is "momentarily" a fixed number, comparable to 12 in the discussion above. We have shown, without using any special properties of k, that 'true for k' implies 'true for (k + 1)' that is $P_k \Rightarrow P_{k+1}$. Now we can say, that it does not matter what k is - the same argument would hold whatever value k has ("this will work for any value of k"). We have made sure that every domino will push over its neighbour - now we have to push over the first one, that is, we have to prove P_1. But P_1 asserts that "$1 = \frac{1.2}{2}$", which is true.

Thus we have proved $P_k \Rightarrow P_{k+1}$ and P_1 } so that the result follows by mathematical induction. (M.I.)

Some further examples follow:-

(j) On page 76 a demonstration is given of the result $1^2 + 2^2 + \ldots n^2 = \frac{n(n+1)(2n+1)}{6}$

A proof by M.I. is as follows:-

(1) To prove $P_k \Rightarrow P_{k+1}$ Assume P_k i.e. $1^2 + 2^2 + \ldots + (k + 1)^2 + k^2 = \frac{k(k+1)(2k+1)}{6}$

Then $1^2 + 2^2 \ldots + k^2 + (k + 1)^2 = \frac{k(k+1)(2k+1)}{6} + (k + 1)^2 =$

$\frac{(k+1)}{6}\left(k(2k + 1) + 6k + 6\right)$

$= \frac{k+1}{6}\left(2k^2 + 7k + 6\right) = \frac{(k+1)(k+2)(2k+3)}{6}$ i.e. P_{k+1} is true.

(2) To prove P_1 we have to verify that $1^2 = \frac{1.2.3}{6}$, which is so.

Since we have proved $P_k \Rightarrow P_{k+1}$ and P_1 } the result follows.

(k) If $x > -1$, $(1 + x)^n \geq 1 + nx$, $n = 1, 2, 3, \ldots$

P_1 states $1 + x \geq 1 + x$ which is true

Assume P_k, i.e. that $(1 + x)^k \geq 1 + kx$

Then $(1 + x)^{k+1} = (1 + x)(1 + x)^k \geq$

$(1 + x)(1 + kx) = 1 + \overline{k + 1}x + kx^2 \geq 1 + \overline{k + 1}x$, since $kx^2 \geq 0$

Hence $P_k \Rightarrow P_{k+1}$ and P_1 } so the result follows by M.I.

Note: The result implies that $(1 + x)^n \geq nx$, $x > -1$, $n = 1, 2, 3 \ldots$ but this cannot be proved directly by M. Induction. P_{k+1} is less demanding, and so should be 'easier to prove' - but P_k is a weaker foundation on which to base the step to P_{k+1} (See Polya (1952) p. 119)

Further examples and Exercises are given in Appendix IIIB, page 79.

Interlude Forming negations of statements. 'For all k, if k is an integer, then 2k + 1 is odd'. We can express this concisely using the symbol $\forall_x$, read as "for all x":-

$\forall_k$, k integer $\Rightarrow$ 2k + 1 is odd .

Such a symbol is called a quantifier - it tells us something about the range of values of the variable to which a statement refers. Another such quantifier is $\exists$ which means "there exists ... such that"...

Thus, "x is odd" $\Leftrightarrow$ "$\exists$ k such that k is an integer and x = 2k + 1"

These symbols help us to express more clearly what we mean. The order in which they are used is important; notice, for example, the difference between $\forall x, \exists y , y > x$ (1)

and $\exists y, \forall x , y > x$ (2) (where x and y are integers)

(1) asserts that given any number x, we can always find a larger number y, whereas (2) asserts that there is a certain number y, which is bigger than any other number. (Consider the effect of leaving out the word 'certain' in the last sentence).

In analysis we use statements like:-

"$\forall \varepsilon > 0, \exists \delta > 0$ such that P is true", where P is some assertion, (which may appear more familiar as "to each $\varepsilon > 0$ there corresponds a $\delta > 0$ . . .")

The negation of the statement is

"for some $\varepsilon > 0$ there does not exist $\delta > 0$ such that P is true"

i.e. "$\exists \varepsilon > 0$ such that $\forall \delta > 0$, P is false". Thus the negation of "$\exists x$, P is true" is "$\forall x$, P is false", and the negation of "$\forall x$, P is true" is "$\exists x$, P is false".

Exercise 9

9.1 Translate into English a) $\forall x$, x is not the brother of y.

b) $\exists z$, z is the sister of y.

c) $\exists x$, x integer, $x^2 = y$

d) $\forall x$, x rational $\Rightarrow x^3 \neq 2$.

9.2 Form the negation of each statement in 9.1. Are any of these necessarily false?

9.3 If x, y, z are positive integers, consider the statements

a) $\forall x \ \exists y \ \exists z , \ x^2 + y^2 = z^2$

b) $\exists y \ \forall x \ \exists z , \ x^2 + y^2 = z^2$

Are they true, or false?

9.4 Let S be the set $\{0, 2, 4\}$. Determine whether each of the following is true or false:-

(a) $\forall x \in S, \ (x + 1)^2 = x^2 + 1$

(b) $\exists y \in S, \ y^2 + y = 6$

(c) $\exists z \in S, \ z^2 + z \neq 6$

(d) $\forall w \in S, \ w^2 + 3w \neq 28$

(e) $\forall v \in S, \ v^3 - 6v^2 + 8v = 0$

9.5 Form the negation of each of 9.4

9.6 Let A be {Pierre, Jean-Paul} and B be {John, Charles, Stuart}

Explain the meaning of each of:-

(a) $\exists x \in A, \forall y \in B$, x is a pen-friend of y

(b) $\exists x \in A, \exists y \in B$, x is a pen-friend of y

(c) $\forall y \in B, \exists x \in A$, x is a pen-friend of y

9.7 Let M, W be the set of all married men, women, respectively.

State in words the meaning of

(a) $\forall x \in W, \ \exists y \in M$, x is married to y

(b) $\exists x \in W, \ \forall y \in M$, x is married to y

9.8 Let p, q be natural numbers. State which of the following are true

(a) $\exists p, \exists q. \ q = p + 2$

(b) $\exists q, \forall p, \ q = p + 2$

(c) $\forall p, \exists q, \ q = p + 2$

(d) $\forall q, \exists p, \ q = p + 2$

9.9 Form the negation of each of 9.8 .

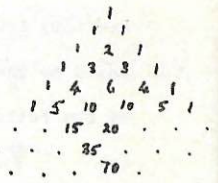
Disproof by Counter-example

This has already been referred to on page 5 , Chapter 1.

Exercise 10 Disprove the following conjectures by finding a counter-example.

10.1 The number of ways of achieving a total of N pence with stamps of value 1p, 2p, 3p is N.

10.2 In Pascal's triangle the sixth row is 1, 5, 10, 10, 5, 1 and the diagonal starting from the fifth row is 1, 5, 15, 35, . . .



This suggests the conjectures

(a) If n is odd the $(n + 1)$th row elements are all divisible by n (except for the 1's at the ends)

(b) If n is prime the elements ${}_nC_1$, ${}_{n+1}C_2$, ${}_{n+2}C_3$ . . . are all divisible by n.

10.3. The binary operation in (i)(2) above is associative. (p. 33).

10.4 $n^k - n$ is divisible by k,

(a) for all k

(b) for k = 2 and for k odd

10.5 Any natural number is the sum of three squares .

10.6 The conjecture (b) of Exercise 5.2, p14.

Other counter-examples already met include Fermat's conjecture (page 5) and the "prime number function" (page 3). An interesting one quoted in the Open University text, Logic II (Unit 17, p.36) is a disproof of the conjecture "Every odd integer is expressible as $p + 2a^2$, where p is a prime" e.g. $9 = 7 + 2.1^2$, $35 = 17 + 2.3^2$ etc. But 5777 cannot be expressed thus, (the proof is by exhaustion).

Indirect proof

Sometimes we show $P \Rightarrow Q$ by assuming $\sim Q$ and obtaining a contradiction. This is equivalent to proving the contrapositive statement $\sim Q \Rightarrow \sim P$.

As an example, we consider the problem of expressing odd integers in the form $x^2 + y^2$. We note that $13 = 2^2 + 3^2$, $17 = 4^2 + 1^2$, $5 = 2^2 + 1$, but that 7, 11, are not expressible in this form. From these observations we may conjecture that numbers of the form $4k + 1$ are expressible in the form $x^2 + y^2$ and numbers of the form $4k + 3$ are not expressible in the form $x^2 + y^2$. Consider the second assertion, which we write as $P \Rightarrow Q$, where :-

P: $N = 4k + 3$

Q: $N \neq x^2 + y^2$

This is most easily proved in the contrapositive form $\sim Q \Rightarrow \sim P$.

Assume $\sim Q$. i.e. $N = x^2 + y^2$. Clearly, if N is odd, one of x, y must be odd, the other even. Let $x = 2a + 1$, $y = 2b$.

$x^2 + y^2 = 4a^2 + 4a + 1 + 4b^2$ of form $4n + 1$ i.e. $\sim P$.

So $\sim Q \Rightarrow \sim P$ i.e. $P \Rightarrow Q$.

The first assertion is the converse of this. i.e. $Q \Rightarrow P$:-

N odd, not of the form $x^2 + y^2 \Rightarrow N = 4k + 3$; and this, though also true, requires a more substantial basis of theory for its proof.(Sierpinski(1964), p.65)

Exercise 11.

11.1 Fermat numbers. Prove that if $N = 2^m + 1$ is prime, then m is of the form 2^k.

11.2 If xy is of form $3k + 2$ then exactly one of x, y is of form $3k + 2$ (x, y integers).

11.3 Let $f: U \to V$ be a linear transformation between vector spaces U,V. The kernel of f, $\ker f$, is the set of elements of U which map on to the zero element of V. Then $\ker f = \{0\} \Leftrightarrow f$ is 1-1.

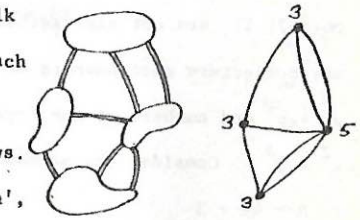
(Prove each part of the implication by an indirect argument.)

CHAPTER 6

PROOFS OF IMPOSSIBILITY AND OF EXISTENCE

We consider first two problems:-

(a) (Euler's "Königsberg bridge problem). Suppose four islands are joined by bridges as shown. Is it possible to walk from island to island in such a way that each bridge is traversed once and only once?



Euler proved the answer is 'no' - as follows. Replace the diagram by an equivalent 'graph', of vertices and arcs, and mark the valency of each vertex. (i.e. the number of arcs meeting there - see page 81). When the path is traced, each 'visit' to a vertex uses up just two of the arcs meeting there. Hence if every arc is traced, each vertex, except those which are start and finish points, must have even valency.

(b) To prove that $\sqrt{2}$ is irrational; i.e. that there do not exist natural numbers a, b such that $\frac{a}{b} = \sqrt{2}$.

(i) We may assume a,b have no common factor, for if by "cancelling down" $\frac{a}{b} = \frac{a_1}{b_1} = \frac{a_2}{b_2}$ . . . . where $a > a_1 > a_2$ . . . the cancelling process must terminate since all the a's are > 0.

(ii) The square of an odd number is odd;- $(2k + 1)^2 = 4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$

Thus if x^2 is even, x is even

Proof. Suppose $\sqrt{2} = \frac{a}{b}$ where a,b have no common factor (by i)

Then $2b^2 = a^2$ so that a^2 is even, $\Rightarrow$ a is even (by ii)

Let $a = 2c$, $a^2 = 4c^2 = 2b^2$ so that b^2 is even, $\Rightarrow$ b is even

Thus a,b have a common factor 2. This contradition establishes the result. (See also Appendix IIIC, page 87).

What is meant by impossibility in a mathematical context.

When it is stated that it is impossible to solve some mathematical problem, some people mistakenly assume that professional mathematicians have collectively admitted defeat, and that a gifted amateur (perhaps themselves!) will succeed where the experts have failed. This is inherently unlikely in the case of an unsolved problem - like 'Fermat's last theorem' (page 70) or, until recently, the 'four-colour conjecture' (see below, p 95) though it is worth noting that Fermat himself was a lawyer and "only" an amateur mathematician. However, it should be clear by now that an impossibility proof demonstrates the logical impossibility of certain circumstances; no amount of ingenuity will 'solve' the Königsberg bridge problem, for a 'solution' would be self-contradictory. If someone produced what was claimed to be a solution, it would hardly be worth while examining it. Nevertheless, although trisecting an arbitrary angle using only 'ruler and compasses' constructions has long been known to be impossible, mathematicians still occasionally receive manuscripts claiming to have solved the problem (sometimes, as in one I received from Australia, with deliberate omission of some sections of the 'proof', for "reasons of security"!)

Existence proofs

(c) A roomful of guests meet at a party; sometimes, when introduced, guests will shake hands.

Prove (i) there are two people who have shaken hands the same number of times.

(ii) the number of people who have shaken hands an odd number of times is even.

(iii) In any set of 6 guests, there are either three who are mutual acquaintances or three who are mutual strangers - i.e. no one of the three knows either of the others.

Proofs (i) Suppose there are k guests, and that there is just one person who has not shaken hands with anybody. Then the others must have shaken hands with, respectively, 1,2, 3, 4 . . (k-1) people. But this is impossible since there are at most (k-2) people who could have shaken hands with the last one. (Similarly, if everyone has shaken hands with someone . . . .).

(ii) Let n_i be the number of handshakes involving the i^{th} person. Then $n_1 + n_2 + \ldots + n_i$ is even (since each handshake is counted twice). Delete all the even terms in this expression - the numbers remaining correspond to people who have shaken hands an odd number of times, and if there were an odd number of terms, the result would be odd.

(iii) We can replace this by an equivalent problem involving arcs joining vertices (a 'graph'). The 6 people are replaced by 6 points (vertices). These are joined in pairs by arcs which are coloured red if the 2 corresponding people are acquaintances, blue, if they are strangers. Then we have to prove there exists either a red or a blue triangle within the graph. Choose any vertex as P, - the five arcs from P, must include 3 (at least) of the same colour - say red - joining to P_i, P_j, P_k. If any one of P_iP_j, P_jP_k, P_kP_i is red, the result follows; if none are, then all are blue . . .

These theorems demonstrate properties which the set of people must possess. In (i) the particular individual(s) is not identified - we know that he (or they) must exist. In (iii) however, the solution not only provides an existence proof, but indicates a method of locating and exhibiting a subset with the desired property - it is a constructive existence proof, whereas (i) was non-constructive. (We could, in principle, locate the

individual concerned in (i) - e.g. by listing - but in some situations this is not possible and the proof may merely tell us that an object exists without telling us how to find it). In Appendix IIIC we give such a non-constructive proof - the famous fixed-point theorem of Brouwer.

Brouwer's proof is essentially non-constructive, giving no procedure for locating the fixed point which it asserts must exist. Concern about possible contradictions arising within mathematics because of the use of non-constructive methods led to the emergence of a school of thought which advocated that only constructive proofs be allowed. It is ironic that one of the leaders of this group was Brouwer, who is perhaps most widely known for his fixed-point theorem, (although he made many other contributions to mathematics, including a constructive proof of the next theorem).

(d) The fundamental theorem of algebra was first proved by Gauss. It asserts that every polynomial equation of degree n with complex number coefficients has/at least one root in complex numbers. It then follows that it has exactly n roots.(†) (See Courant and Robbins, 1941, pp. 101, 269 for proofs of these results.) Note that the fundamental theorem is not true if 'complex' is replaced by 'natural', 'integer', 'rational', or 'real':-

In order to be able to solve $x + 3 = 2$, $3x = 2$, $x^2 = 2$, $x^2 + 1 = 0$ we have to introduce integers, rationals, reals, complex numbers

It might be expected that in order to solve/all polynominal equations involving complex numbers, some 'new' type of number would have to be introduced; Gauss' result shows this is not so.

(†) (with the usual conventions for multiple roots).

(e) The number of primes is infinite

A famous proof is due to Euclid. Let $p_1 \ldots p_n$ be a list of all the prime numbers (assume the list is finite). Consider $N = 1 + p_1p_2p_3 \ldots\ldots p_n$. Evidently N is not divisible by p_1 (since, on division, the remainder is 1) and similarly N is not divisible by p_i for any i. Thus N either is itself prime, or if, composite, it is divisible by some prime not in our list $p_1, p_2, p_3 \ldots p_n$.

CHAPTER 7

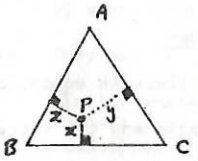
OBTAINING PROOFS. THE USE OF GENERALISATION, SPECIALISATION AND ANALOGY

Most of this chapter is derived from the ideas of G. Polya (whose books "Induction and Analogy" and "Mathematical Discovery" are referred to in the bibliography).

Generalisation and specialisation

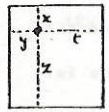
Example (a)

In Ch. 5, p. 32 we considered the problem: "To prove $x + y + z$ = constant", (see fig.). The value of the constant must be $a\sqrt{3}$ - we obtain this by specialising, e.g. by placing P at A. The problem may be generalised in various ways:-

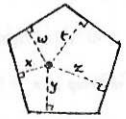


(ΛABC equilateral, side 2a)

First we may consider regular figures with 4, 5, 6, . . . sides:-

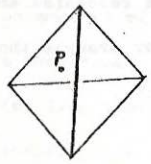


$x + y + z + t$ = constant (trivially)



$x + y + z + t + w$ = const. (by similar proof)

We may also generalise (i) to positions of P outside the Δ (which leads to results like $x + y - z$ = const. etc.) and (ii) to 3 dimensions:-



Regular tetrahedron, interior point P. Perpendicular distances from P to faces x, y, z, t. Then $x + y + z + t$ = constant.

Proof:- by analogy, divide the total volume of the tetrahedron into 4 volumes given by $\frac{1}{3}$(face area) x height.

(e) The number of primes is infinite

A famous proof is due to Euclid. Let $p_1 \ldots p_n$ be a list of all the prime numbers (assume the list is finite). Consider $N = 1 + p_1p_2p_3 \ldots\ldots p_n$. Evidently N is not divisible by p_1 (since, on division, the remainder is 1) and similarly N is not divisible by p_i for any i. Thus N either is itself prime, or if, composite, it is divisible by some prime not in our list $p_1, p_2, p_3 \ldots p_n$.

CHAPTER 7

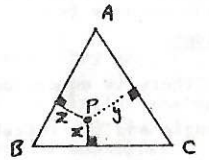
OBTAINING PROOFS. THE USE OF GENERALISATION, SPECIALISATION AND ANALOGY

Most of this chapter is derived from the ideas of G. Polya (whose books "Induction and Analogy" and "Mathematical Discovery" are referred to in the bibliography).

Generalisation and specialisation

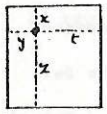
Example (a)

In Ch. 5, p. 32 we considered the problem: "To prove $x + y + z$ = constant", (see fig.). The value of the constant must be $a\sqrt{3}$ - we obtain this by specialising, e.g. by placing P at A. The problem may be generalised in various ways:-

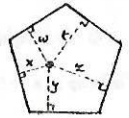


(ΔABC equilateral, side 2a)

First we may consider regular figures with 4, 5, 6, . . . sides:-

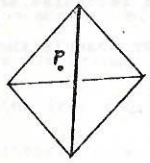


$x + y + z + t$ = constant (trivially)



$x + y + z + t + w$ = const. (by similar proof)

We may also generalise (i) to positions of P outside the Δ (which leads to results like $x + y - z$ = const. etc.) and (ii) to 3 dimensions:-



Regular tetrahedron, interior point P. Perpendicular distances from P to faces x, y, z, t. Then $x + y + z + t$ = constant.

Proof:- by analogy, divide the total volume of the tetrahedron into 4 volumes given by $\frac{1}{3}$(face area) x height.

Clearly in a similar way, we may prove:-

"From a point P within the interior of a regular dodecahedron, perpendiculars are drawn to each of its 12 faces. The sum of the lengths of these 12 perpendiculars is independent of the position of P."

Given at the outset this would appear rather formidable - but less so when set at the end of the above sequence. We can use generalisation to see how to extend solutions of simpler problems to more general (and more difficult) ones, and conversely confronted with a difficult problem, it is often profitable to solve a related simpler problem first.

Analogy

There is an obvious analogy between the two problems involving the triangle and the tetrahedron - analogous results and analogous proofs. Such analogies may suggest ways of solving problems by using methods successful in analogous cases. Polya (1954) gives many examples - e.g. the intersection of a straight line with a set of parallel planes in space, the diagonals of a parallelepiped, the planes which perpendicularly bisect the edges of a tetrahedron - all are immediate 3 D analogues of theorems of plane geometry. He refers also to two classical examples of analogy - that between the fall of an apple, the path of a thrown ball, and of an Earth satellite, and Euler's summation of the series $1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots$ giving the result $\frac{\pi^2}{6}$ by a daring use of analogy (applying polynomial equation theory to the equation $\sin x = 0$).

One powerful method of attack becomes available when we recognise analogies between methods and problems in two areas of mathematics. for example the similarities between finite differences and differentiation:-

The sequence of cubes of natural

numbers is	1	8	27	64	125	216	...
their 1st differences are		7	19	37	61	91	
their 2nd differences are			12	18	24	30	
their 3rd differences are				6	6	6	
their 4th differences are				0	0		

We observe that the 3rd differences of the cubic expression are constant; the 4th differences are zero. The difference sequence of a cubic is quadratic. These are instances of a general theorem - the kth differences of a polynomial of degree k are constant, the (k + 1)th differences are zero. They may be compared with $D(x^k) = kx^{k-1}$, $D^k(x^k) = \text{const.}$, $D^{k+1}(x^k) = 0$. A similar analogy holds between second-order linear differential equations and second-order linear difference equations:-

$(D^2 - 5D + 6)y = 0$ $\qquad$ $u_{n+2} - 5u_{n+1} + 6u_n = 0$

$y = Ae^{3x} + Be^{2x}$ $\qquad$ $u_n = A.3^n + B.2^n$

In each case the "auxiliary equation" is $m^2 - 5m + 6 = 0$

$m = 2$ or 3. (See Exercise 13, p61).

There are many other such analogies at all levels - between the properties of Laplace transforms (for solving differential equations) and of characteristic functions (in statistical theory); between electrical and mechanical oscillations; between the equation $S^2 = \frac{\sum x^2}{n} - \left(\frac{\sum x}{n}\right)^2$ and the parallel axis theorem on moments of inertia. In some cases the underlying similarities give rise to a new branch of mathematics, as with group theory, which arose as an abstraction from approaches common to several apparently unconnected areas (number theory, geometrical symmetry, crystallography), or linear algebra, which unifies work on matrices, geometrical transformations, statistical theory, systems of linear equations and of differential equations, and so on. (See Fletcher (1972)).

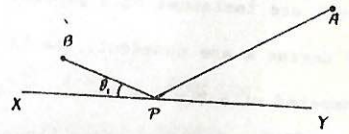
It is worth remarking that analogies can sometimes be misleading:- Moses (1974) p.122 remarks that Euler's "daring conjecture" would have failed for $e^x \sin x = 0$; the analogy between finite sums and infinite series is shown to break down (Appendix III D, 9,10,11); some results in 2 dimensions have no analogue in 3 dimensions. (See Appendix III A 2 on equidecomposable figures).

Physical analogies

Polya (1954) gives many examples where the solution of a mathematical problem is suggested by argument from physical situations:-

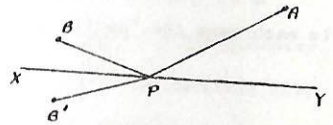
Examble (b)

Find the shortest path APB if P lies on the line XY. You may have met the general physical principle that the path of a ray of light from A to B is such as to make the time of travel from A to B a minimum.



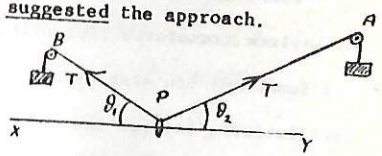
This suggests that the light ray will "solve our problem for us" - the angles $\widehat{BPX}$, $\widehat{APY}$ will be equal ($\theta_1 = \theta_2$) by the law of reflection. We may also be led to think of B′ the image of B in the 'mirror' XY.

Now a 'normal' geometrical proof emerges; BP = B′P, and B′P + PA is evidently least when B′PA is a straight line . . .



But - it was the analogy of the light ray which suggested the approach.

An alternative mechanical analogue may be used which also suggests that $\theta_1 = \theta_2$, though it gives no hint of the usefulness of introducing B′. A string passes over pulleys at A and B and carries equal masses at each end. At P it is attached to a ring which slides along the smooth horizontal rod XY. At the equilibrium position (i) BP + PA will be a minimum (so that the centre of gravity of the system is as low as possible).

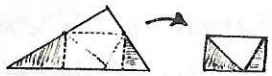


(ii) $T \cos \theta_1 = T \cos \theta_2$, i.e. $\theta_1 = \theta_2$

(Considering the horizontal equilibrium of the ring, the tension of the string being T)

Other physical demonstrations of mathematical theorems are given in Courant and Robbins (1941) (pp.385-97 - using soap films to solve minimum problems, including that of Exercise 12.2 below). Hardy, Littlewood and Polya, in their "Inequalities" (1934) C.U.P. p.262 give a mechanical illustration of a theorem; If $0 \leq a_1 \leq a_2 \leq a_3 \ldots \leq a_n$, $0 \leq b_1 \leq b_2 \ldots \leq b_n$, then Σab is greatest when the a's and b's are paired in corresponding order, (for if the a's are distances and the b's weights, "we get maximum statical moment when we hang the heaviest weights on the hooks farthest from the end").

Paper-folding can also be used to demonstrate elementary geometrical results - the concurrency of the medians of a triangle, and the area of a triangle (see fig.) but note that it also 'demonstrates' the false result of Exercise 5.2, p14.

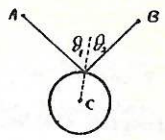


Exercise 12

12.1. Show that $u_n = At^n$, where A is a constant and $t = \frac{1 \pm \sqrt{5}}{2}$, satisfies $u_{n+1} = u_n + u_{n-1}$. Hence show that a solution satisfying $u_1 = u_2 = 1$ is $u_n = \frac{1}{5}(\alpha^n - \beta^n)$ where $\alpha = \frac{1 + \sqrt{5}}{2}$, $\beta = \frac{1 - \sqrt{5}}{2}$.

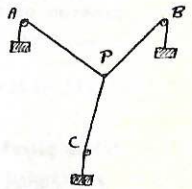
12.2. ΔABC is acute angled. Find the position of a point P inside it such that AP + PB + PC is least.

Hints (for a variety of solutions)

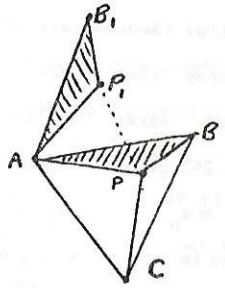


(α) If PC is held constant, find P so that AP + PB is least.

(β) Consider 3 strings joined at P, each with equal masses at their ends, passing over pulleys at A,B,C.



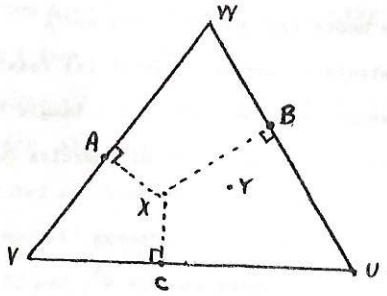
(γ)



Rotate Δ APB thro' 60°.

Show AP + BP + PC = $B_1P_1 + P_1P + PC$.

(δ)



Draw equilateral ΔUVW with sides through A,B,C, $\perp$ AX,BX,CX, (where X is the point such that AX,BX,CX meet at 120°). Let Y be any other point. Then

AX + BX + CX < AY + BY + CY.

(Use the result of Chapter 5, Example f, p. 32.).

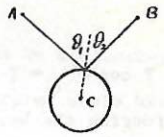
APPENDIX I

AXIOMATIC REASONING

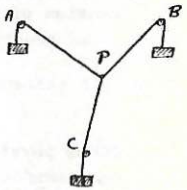
We noted earlier that proofs involving diagrams may sometimes be misleading, for they may involve hidden assumptions of which we are not aware. (See pp. 13,14,55). In order to make all assumptions quite explicit and clearly identifiable, mathematicians have developed axiomatic proof, in which every statement is a logical consequence of the axioms, together with any statements subsequently proved, and of these alone. Thus anyone who accepts the axioms is bound to accept their consequences as deduced. Initially - e.g. as in the work of Euclid - axioms were regarded as starting points, 'self evident truths' upon which everyone could be expected to agree. Today the word 'postulates' is sometimes used to describe initial assumptions. It is not necessary that these be 'true' and they may not apply to any physical objects in the real world; although they must be self consistent (see below). Nevertheless, if they are accepted, any deductions made from them must also be accepted. Where the axioms of Euclid referred to straight lines, points, etc., the counterparts of physical objects, the postulates of a mathematical theory may refer to undefined objects whose properties are those specified by the postulates, and no others. (See the example (a) in the Appendix II, p62). It may be helpful to think about the theory in terms of an 'interpretation' or 'model' - e.g. by regarding the 'lins' and 'poins' of the postulates as lines and points respectively - but all proofs must be independent of such interpretations and given solely in terms of the postulates.). The use of undefined terms and of postulates which are not asserted as true, led Bertrand Russell to describe mathematics paradoxically as a study in which "we neither know what we are talking about nor care if it is true".

Hints (for a variety of solutions)

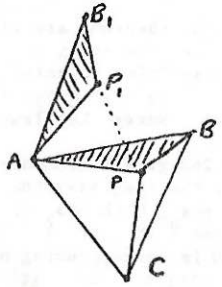
(α) If PC is held constant, find P so that AP + PB is least.



(β) Consider 3 strings joined at P, each with equal masses at their ends, passing over pulleys at A,B,C.



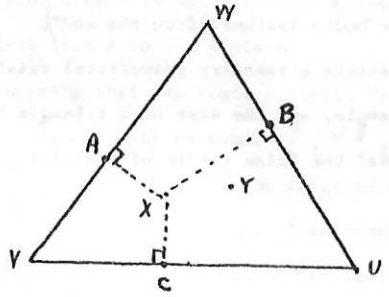
(γ)



Rotate Δ APB thro' 60°.

Show AP + BP + PC = $B_1P_1 + P_1P + PC$.

(δ)



Draw equilateral ΔUVW with sides through A,B,C, $\perp$ AX,BX,CX, (where X is the point such that AX,BX,CX meet at 120°). Let Y be any other point. Then

AX + BX + CX < AY + BY + CY.

(Use the result of Chapter 5, Example f, p. 32).

APPENDIX I

AXIOMATIC REASONING

We noted earlier that proofs involving diagrams may sometimes be misleading, for they may involve hidden assumptions of which we are not aware. (See pp. 13,14,55). In order to make all assumptions quite explicit and clearly identifiable, mathematicians have developed axiomatic proof, in which every statement is a logical consequence of the axioms, together with any statements subsequently proved, and of these alone. Thus anyone who accepts the axioms is bound to accept their consequences as deduced. Initially - e.g. as in the work of Euclid - axioms were regarded as starting points, 'self evident truths' upon which everyone could be expected to agree. Today the word 'postulates' is sometimes used to describe initial assumptions. It is not necessary that these be 'true' and they may not apply to any physical objects in the real world; although they must be self consistent (see below). Nevertheless, if they are accepted, any deductions made from them must also be accepted. Where the axioms of Euclid referred to straight lines, points, etc., the counterparts of physical objects, the postulates of a mathematical theory may refer to undefined objects whose properties are those specified by the postulates, and no others. (See the example (α) in the Appendix II, p62). It may be helpful to think about the theory in terms of an 'interpretation' or 'model' - e.g. by regarding the 'lins' and 'poins' of the postulates as lines and points respectively - but all proofs must be independent of such interpretations and given solely in terms of the postulates.). The use of undefined terms and of postulates which are not asserted as true, led Bertrand Russell to describe mathematics paradoxically as a study in which "we neither know what we are talking about nor care if it is true".

We give first some further examples which illustrate the need for care in avoiding hidden assumptions.

(a) If $a_n > b_n$ for all n, we might expect $\lim(a_n) > \lim(b_n)$ as $n \to \infty$.

But let $a_n = \frac{1}{n}$, $b_n = \frac{1}{2n}$, Then $a_n > b_n$, all n, but $\lim(a_n) = 0 = \lim(b_n)$

The correct conclusion is $\lim(a_n) \geq \lim(b_n)$.

(b) Since $x + y + z = x + z + y$, etc. we might expect that <u>infinite</u> sums could be similarly re-arranged.

But consider $S_1 = 1 - 1 + \frac{1}{2} - \frac{1}{2} + \frac{1}{3} - \frac{1}{3} \ldots$ which is cgt. with sum = 0,

and $S_2 = 1 + \frac{1}{2} - 1 + \frac{1}{3} + \frac{1}{4} - \frac{1}{2} + \ldots \left(\frac{1}{2m-1} + \frac{1}{2m} - \frac{1}{m}\right) + \ldots$ ($3m$ terms)

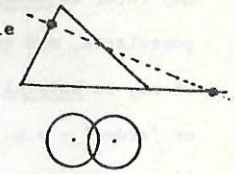
$(S_2)_{3m \text{ terms}} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots \ldots + \frac{1}{2m-1} + \frac{1}{2m}$

$-(1 + \frac{1}{2} + \frac{1}{3} \ldots + \frac{1}{m}) = \frac{1}{m+1} + \frac{1}{m+2} + \ldots \frac{1}{2m} > m \cdot \frac{1}{2m} = \frac{1}{2}$

Thus S_2 is either cgt. with sum $\geq \frac{1}{2}$ or is divergent.

More generally it can be shown that care is needed when dealing with infinite series - such operations as multiplying, differentiating or integrating term by term may sometimes lead to erroneous results, so that the circumstances under which these <u>are</u> valid need to be investigated.

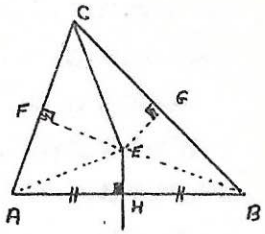
(c) The axiom system of Euclid's geometry, though one of the great achievements in mathematics, contains some imperfections. In particular, there are no axioms of order or "betweenness", such as those which would allow us to conclude that a line which meets one side of a triangle and another side produced, must also meet the third side, or that two equal circles whose centres are separated by a distance of less than their diameter, must intersect.†



It may be objected that these matters are "obvious from the diagram", but this is a dangerous argument, as the following example shows.

† The assumption that the circles intersect is the first 'flaw' in the 'Elements' - it occurs in Proposition 1.

<u>To prove that any triangle is isosceles</u>



<u>Given</u>: any triangle ABC.

<u>Construction</u>: Draw the bisector of $\widehat{ACB}$ and the perpendicular bisector of AB. From their pt. of intersection, E, draw perpendiculars EG, EF to the sides BC, CA, respectively, and join AE and BE.

<u>Proof</u>: Δ's AEH, BEH are congruent since EH is common, AH = HB, $\widehat{EHB} = \widehat{EHA} = 90°$ hence AE = BE and $\widehat{EAH} = \widehat{EBH}$

Δ's CFE, CGE are congruent, $\begin{cases} \widehat{FCE} = \widehat{GCE} \text{ (EC bisects FCG)} \\ \text{CE is common} \\ \widehat{EFC} = \widehat{EGC} = 90° \end{cases}$

hence EG = EF.

Δ's AEF, BEG are congruent since EG = EF (proved)

AE = EB (proved)

$\widehat{EFA} = \widehat{EGB} = 90°$

hence $\widehat{FAE} = \widehat{GBE}$

From above $\widehat{EAH} = \widehat{EBH}$

so that $\widehat{FAE} + \widehat{EAH} = \widehat{GBE} + \widehat{EBH}$

that is $\widehat{CAB} = \widehat{CBA}$,

<u>so the triangle is isosceles</u>.

(For interested readers, a full discussion of this paradox is given in Northrop, E. (1944) <u>Riddles in Mathematics</u>. Penguin Books, pp. 98-102.)

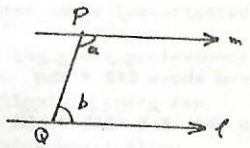
<u>The reasons for the axiomatic approach</u>

It is evident that care is needed if fallacies are to be avoided; it is not mere pedantry which makes mathematicians insist upon rigorous standards of proof. Following the development of axiomatic treatments, it was realised that a further benefit arose, that of economy through abstraction.

When we develop a theory of abstract vector spaces, the results we obtain are valid for any collection of objects and operations which satisfy the axioms or postulates (see *Exercise 13*, p. 61); thus at one stroke we obtain results which apply to vectors, polynomials, functions satisfying certain differential equations, and so on. Further, ideas and methods used in one branch of mathematics can suggest corresponding results in other related branches. It is therefore sensible, in terms of unifying and simplifying the structure of mathematics, to prove theorems 'once and for all' in abstract axiomatic terms - though this may not be the best way to approach the subject matter for the first time as a learner.

The modification of axiom systems may occasionally generate new and interesting results, (although frequently the outcomes are worthless). Perhaps the most famous instance of this is the investigation of Euclid's 5th postulate, which led ultimately to the realisation that other (non-Euclidean) geometries could exist, in which this postulate does not hold.

Euclid's 5th postulate asserts: "if $a + b < 180^\circ$ the lines ℓ, m will meet, if produced, on the same side of PQ as are *the angles a, b*".



This may be shown to be equivalent to :-
"if the lines do not meet, then $a + b = 180^\circ$"
and "there is a unique parallel to ℓ through P".

In the hyperbolic geometry of Gauss, Lobachevsky and Bolyai, there are an infinite number of lines through P which do not meet ℓ, (and the sum of the angles of a triangle is $<180^\circ$); in Riemann's elliptic geometry there is no line through P which does not meet ℓ (and the angle sum of a triangle is $>180^\circ$) (Courant and Robbins (1941), p.222).

Finally the properties of axiom systems themselves have become an object of study within mathematics, as part of the Foundations of Mathematics. We may ask of any axiom system whether it is consistent, complete, and whether the axioms are independent. A consistent system is one in which no contradiction can be proved. In the days when axioms were regarded as 'self-evident truths', there was less worry about the possibility of an axiom system being self-contradictory; but if the postulates are deliberately divorced from the physical world, this can no longer be excluded. Whilst it is easy to avoid obviously incompatible postulates (such as "(1) all elements of S are even", "(2) all elements of S are odd", "(3) the number of elements of S is not zero"), it is not possible to forsee all the consequences of an arbitrary set of postulates which might prove mutually contradictory. In general it is not possible to prove consistency (though see Hilbert's proof, Appendix II, 9, p.70), and the usual check is to ask whether postulates are satisfiable, i.e. whether there exists a model (or set of objects of which the postulates are true - and which therefore implies their consistency).

An independent axiom is one which is not deducible from the other axioms. Thus the 5th postulate of Euclid, was eventually proved to be independent (by exhibiting a model in which all other axioms were satisfied and the parallel axiom was not), after many failures to deduce it from his other axioms.

A complete system is one in which no new independent axiom exists - i.e. every statement of the system may either be proved true or proved false. Again it is impossible to determine this in general, since it is tantamount to being able to decide the status of all theorems. Instead we may ask whether a system is categorical, i.e. whether any two models of the system are necessarily isomorphic.

An example of a simple axiom system together with illustrations of these concepts is given in Appendix II, p.67. We turn now to some examples of axiomatic treatments of the arithmetic of integers and of natural numbers.

(d) Given that the real numbers a,b,c . . . satisfy the postulates below, prove;-

$\forall a, b$,

(i) $a.0 = 0$,

(ii) $a.(\bar{}b) = \bar{}(a.b)$,

(iii) $(\bar{}a).(\bar{}b) = (a.b)$.

Postulates:- $\forall a, b, c$:-

(1) $a + b$ *is* a real number (Closure)

(2) $(a + b) + c = a + (b + c)$ (Associative)

(3) $a + 0 = a = 0 + a$ (Identity)

(4) $a + \bar{}a = 0 = \bar{}a + a$ (Inverse)

} Group under $+$

(5) $a + b = b + a$

(6) $a.b$ *is* a real number

(7) $(a.b).c = a.(b.c)$

(8) $a.(b + c) = a.b + a.c$ and (8)' $(b+c).a = b.a + c.a$

} *Ring.*

The properties 1-8 are (some of) the well-known properties of the real numbers; we use them to deduce others.

(Note: 0 is categorised (in 3) as the identity for addition but (i) above is a multiplicative property. Likewise, (ii) and (iii) exhibit the interrelations between performing multiplication, and finding inverses with respect to addition).

Proofs. $\forall a, b$:-

(i) $a.b \overset{3}{=} a.(b + 0)$

$\overset{8}{=} a.b + a.0$

$\exists c$ s.t. $c \overset{6}{=} a.b$

Hence $\bar{}c \overset{4}{=} \bar{}(a.b)$.

$\therefore \bar{}c + a.b = \bar{}c + (a.b + a.0)$

$\overset{2}{=} (\bar{}c + a.b) + a.0)$

$\therefore 0 \overset{4}{=} 0 + a.0$

$\therefore \underline{0 \overset{3}{=} a.0}$

(ii) $0 \overset{(i)}{=} a.0 \overset{4}{=} a(b + \bar{}b) \overset{8}{=} a.b + a.\bar{}b$

Let $d = \bar{}(a.b)$ (6 and 4)

then $d + 0 = d + (ab + a.\bar{}b)$

$\overset{2}{=} (d + ab) + a.\bar{}b$

$\therefore d \overset{3}{=} 0 + a.\bar{}b$

$\therefore \underline{\bar{}(a.b) \overset{3}{=} a.\bar{}b}$

$\forall a, b$

(iii) $(a + \bar{}a).\bar{}b \overset{4}{=} 0.\bar{}b = 0$ (by analogue of (i), deduced from (8)')

$\therefore a.\bar{}b + \bar{}a.\bar{}b \overset{8}{=} 0$

$\therefore \bar{}(a.b) + \bar{}a.\bar{}b \overset{(ii)}{=} 0$

$\therefore \underline{\bar{}a.\bar{}b \overset{3}{=} a.b}$

Note: If we also assume (9) . . . $a.b = b.a$, then (8)' follows from (8).
(For a proof that (8) and (8)' do not imply (9), see Richards, A. Math. Gaz. 413, p205 (1976)).

(e) Define the integers x,y,z, . . . as classes of ordered pairs of natural numbers, $x = (a,b)$ $y = (c,d)$ . . .

with the following definitions:-

(1) Equality $x = y$ iff $a + d = b + c$

(2) Addition $x + y = (a + c, b + d)$

(3) Multiplication $x.y = (ac + bd, ad + bc)$

Note It may help to make the definitions more intelligible if we think of x as represented by the result of $(a - b)$. e.g. the integer $\bar{}3$ is represented by (8,5) or (7,4), whereas (5,8), (4,7), etc. represent the integer $\bar{}3$.

(Strictly, it is necessary to show that equality as defined in (1) has the usual reflexive, symmetric and transitive properties, and that addition and multiplication are well-defined by (2) and (3) - i.e. that the results of $x+y$ and xy are independent of the particular pairs chosen to represent x and y. However, we shall assume these properties, which are not difficult to verify. We shall also assume all properties of natural numbers as required.)

Prove: (i) $\exists$ 0 such that $x + 0 = x$, ($\exists$ = "there exists")

(ii) $\exists\ \bar{}x$ such that $x + \bar{}x = 0$,

(iii) $\bar{}x.y = \bar{}(x.y)$,

(iv) $\bar{}x.\bar{}y = x.y$.

Proofs: (We omit details in (ii) and (iii))

(i) Take 0 as (p,p) for any p, and $x = (a,b)$.

Then $x + 0 \overset{2}{=} (a + p, b + p)$

and $(a + p, b + p) \overset{1}{=} (a,b)$ since $a + p + b = b + p + a$

by properties of natural numbers

(ii) Take $\bar{x}$ as (b,a)

(iii) ——

(iv) Take y as (c,d.), $\bar{y}$ = (d,c)

$-x \,.\, -y = (b,a) \,.\, (d,c)$

$\overset{3}{=}$ (bd + ac, bc + ad)

and $x.y \overset{3}{=}$ (ac + bd, ad + bc)

and these are equal[1] iff

(ac + bd) + (bd + ad) = (bd + ac) + (ad + bc)

which is true by properties of natural numbers.

Comments

In a similar way, rationals may be defined as ordered pairs of integers, and complex numbers as ordered pairs of reals. The real numbers are more troublesome to handle, but may be treated axiomatically by the method of 'Dedekind cuts' or 'nested intervals' applied to the set of rational numbers. (See Wheeler (1974)).

Thus the whole structure of relationships between numbers of all types. can be put on an axiomatic basis. This is not to say that we should do arithmetic or perform calculations axiomatically - it means, for example, that if we are satisfied that the rules we use for dealing with the natural numbers are consistent, then so are those for real and complex numbers, and, by an extension, so are the theorems of analysis - on series, differentiation, integration etc. - which rest upon these. Indeed, since geometry can be dealt with in terms of coordinates we see emerging the possibility of placing the whole of mathematics on an axiomatic basis, of which the arithmetic of natural numbers is the foundation. If this were done, we should have made mathematics into a harmonious whole, but more importantly, it might prove possible to demonstrate conclusively that mathematics is logically self-consistent, with no possibility of contradiction arising within it. This task was attempted by Hilbert and others, with some success, but the ultimate objective, of proving mathematics consistent, was eventually proved to be unattainable by Gödel - an impossibility

proof concerning the nature of mathematics itself. This is a very subtle matter, of which some account is given in Appendix II following.

Exercise 13

The axioms for a linear vector space are as follows:-

A vector space V (over the real numbers) is a set of objects (called vectors) $\underline{x}, \underline{y}, \underline{z}$ . . . satisfying the following:-

(1) To every pair $\underline{x} \in V, \underline{y} \in V$ there corresponds a vector $\underline{x} + \underline{y}$ such that (V,+) is a commutative group.

(2) To every pair $\lambda \in \mathbb{R}$, $\underline{x} \in V$ there corresponds a vector $\lambda\underline{x} \in V$ such that, $\forall\ \underline{x}, \underline{y}, \lambda, \mu$:-

(i) $\lambda(\underline{x} + \underline{y}) = \lambda\underline{x} + \lambda\underline{y}$,

(ii) $\lambda(\mu\underline{x}) = (\lambda\mu)\underline{x}$,

(iii) $1.\underline{x} = \underline{x}$

Verify that (a) vectors in the plane,

(b) real polynominals of degree ≤ 3,

(c) the family of functions $Ae^{x} + Be^{2x} + Ce^{3x}$, all of which satisfy the differential equation $(D^3 - 6D^2 + 11D - 6)y = 0$,

are structures which each satisfy the axioms under their usual operations.

APPENDIX II

AXIOMATICS AND THE FOUNDATIONS OF MATHEMATICS

We begin with some examples of axiom systems, including Peano's axioms for the natural numbers, which play a major role in what follows.

(a) An Example of an Axiom System - adapted from Blumenthal, (1961), p44.

Set P of "poins" p,q,r, ... Set L of "lins" λ, μ, ν (which are themselves subsets of P).

Postulates or Axioms

1) $\forall p,q \in P,\ p \neq q,\ \exists$ at least one $\lambda \in L$ s.t. $p \in \lambda$, $q \in \lambda$.

2) $\forall p,q \in P,\ p \neq q,\ \exists$ at most one $\lambda \in L$ s.t. $p \in \lambda$, $q \in \lambda$.

3) $\forall \lambda, \mu \in L,\ \lambda \neq \mu,\ \exists$ at least one $p \in P$ s.t. $p \in \lambda$, $p \in \mu$.

4) L is not empty.

5) $\forall \lambda \in L,\ \exists$ at least three distinct elements in λ

6) $\forall \lambda \in L,\ \exists p \in P$ s.t. $p \notin \lambda$.

7) $\forall \lambda \in L,\ \exists$ at most three distinct elements in λ

Models of this axiom system

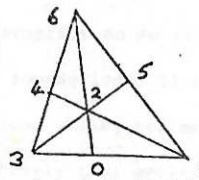
I 'Poins' are the set $\{A, B, C, \ldots G\}$

A B C D E F G
B C D E F G A
D E F G A B C

'Lins' are columns of the array (7 lins)

e.g. (ABD) is a 'lin'.

II



'Poins' are pts. with numbers.

'Lins' are the collinear triples, plus the triple (0,4,5).

Exercise (a) Verify that models (i) and (ii) satisfy all the axioms

(b) Determine which axioms are satisfied by the models below:-

(i) P is set $\{A,B,C,D.E\}$. L is set of 2 'lins' (ABC) and (ADE).

(ii) P is $\{A,B,C,D\}$, L is set (ABC), (ABD), (ACD).

(iii) P is $\{A,B,C\}$, L is set (AB), (BC), (AC).

(iv) P is $\{A,B,C\}$, L is (ABC) [one 'lin'].

(v) P is set of all lines in 3D space thro' pt. O. L is set of all planes thro' O.

(vi) P is set $\{A,B,C, \ldots, M\}$, L is set of columns of array:-

A B C D E F G H I J K L M

B C D E F G H I J K L M A

E F G H I J K L M A B C D

G H I J K L M A B C D E F

Theorems

(A) $p,q \in P,\ p \neq q \Rightarrow$ exactly one $\lambda \in L$ s.t. $p \in \lambda$, $q \in \lambda$. (Axioms 1 & 2).

(B) $\lambda, \mu \in L,\ \lambda \neq \mu, \Rightarrow$ exactly one $p \in P$ s.t. $p \in \lambda$, $p \in \mu$ (Ax 3 & Thm A).

(C) $\exists$ poins p,q r $\in$ P all distinct not all $\in$ same λ, $\lambda \in L$.

Proof By ax. 4,5, $\exists \lambda$ denoted by (ABD). By ax. 6, $\exists$ poin C not $\in \lambda$. Thus A,B,C are distinct and not all $\in$ same lin λ

(D) The set P contains at least 7 elements.

Proof By (C) $\exists$ lin (ABD) and C not on it

By (A) $\exists$ lin (BCE) and E $\neq$ B,C,A, or D.

& $\exists$ lin (DCF) and F $\neq$ D,C,A,B, or E.

& $\exists$ lin (EDG) and G $\neq$ E,D,A,B,C,F.

$\therefore$ $\exists$ at least 7 distinct poins - viz. ABCDEFG.

(F) The set P contains exactly 7 elements and is isomorphic to models I and II.

Exercise Prove (E) - see below(c).

(b) Russell's set Paradox

An everyday version of this concerns "the village barber who shaves everyone in the village who does not shave himself." The problem is, who shaves the barber? Whichever option we take we arrive at a contradiction; we conclude that the notion of such a barber is self-contradictory - he cannot exist.

Russell notes that sets can have as members other sets, and that some sets can be members of themselves. (The set of all abstract ideas is itself an abstract idea).

We exclude such sets as extraordinary, and consider the set S of all ordinary sets - i.e. sets which are not members of themselves. Then

S ordinary $\Rightarrow$ S not a member of itself $\Rightarrow$ S not included among the ordinary sets $\Rightarrow$ S extraordinary.

S extraordinary $\Rightarrow$ S a member of itself $\Rightarrow$ S belongs to the set of ordinary sets $\Rightarrow$ S ordinary.

Thus S is a self-contradictory notion; yet the idea of 'set' and 'belonging to a set' seems intuitive ("What these ideas mean it is necessary to know if you wish to become an arithmetician. But nothing is easier than that." wrote Russell in 1901, before discovering the Paradox). Frege used them as the basis of an attempt to model the natural numbers, from which the 'self-evidently true' nature of arithmetic would follow; Russell's Paradox destroyed this hope.

(c) Further discussion of the axiom system of (a) above (adapted from Blumenthal, (1961)).

Proof of (E):- Suppose $\exists$ another poin H ($\neq$ A,B,...G). Then, by Thm (A), $\exists$ lin (AHX). This has a poin in common with (BCE), with (DCF), and with (EDG), by Thm (B).

X = C or E
X = C or F
X = E or G

are all simultaneously true, which is impossible. Thus H does not exist, and there are exactly 7 poins.

There will be lins (EFP), (FGQ), (GAR), with P $\equiv$ A (cannot be B,C,D,G, $\therefore$ = A).

Q $\equiv$ B, R $\equiv$ C, which shows system isomorphic with model I.

The system is a finite projective geometry, denoted by 7_3

Proofs of Independence

Model (i) satisfies axioms 2-7, not 1 , $\therefore$ 1 is independent
" (ii) " " 1,3-7, not 2 , $\therefore$ 2 " "
" (iii) " " 1-4,6,7, not 5, $\therefore$ 5 " "
" (iv) " " 1-5,7, not 6 , $\therefore$ 6 " "
" (v) " (vi) } satisfy 1-6, not 7 , $\therefore$ 7 is independent

Thus axioms 1,2,5,6,7 are independent. ($\exists$ models to show independence of 3 and 4).

Examination of axiom system 7_3

(a) Satisfiable? - yes, $\exists$ models I and II.

(b) All 7 axioms are independent.

(c) Categorical? - yes, by theorem (E) any model is isomorphic to I.

(Note that the system of axioms 1,2,3,4,5,6, $\sim$7 is not categorical, for models (v) and (vi) both satisfy these axioms, but (v) has ∞ elements, while (vi) is the finite projective geometry 13_4 with 13 elements; hence (v) and (vi) are not isomorphic).

(d) Peano's axioms

These enable us to deduce the usual properties of the natural numbers, among which are the analogues of (1), (2), (5), (6), (7), (8) of example (d), App I, p 58, (referring to real numbers).

The Peano axioms refer to a set $\mathbb{N}$ of elements x, with an undefined relation S (the successor). (It is helpful to regard S(x) as "x + 1").

The following assumptions are made:-

(1) $\exists$ $1 \in \mathbb{N}$ and S(x) = 1 is false, all x.

(2) $x \in \mathbb{N} \Rightarrow S(x) \in \mathbb{N}$ and is unique.

(3) $S(x) = S(y) \Rightarrow x = y$.

(4) If, for some subset $G \subset \mathbb{N}$, $1 \in G$ and $(x \in G \Rightarrow S(x) \in G)$

then $G \equiv \mathbb{N}$. (The Postulate of Mathematical Induction).

We give below definitions for addition and multiplication, and proofs of two theorems (corresponding to (2) and (5) of p.58 above).

Definition $x + 1 = S(x)$

$x + S(y) = S(x + y)$

Theorem $(x + y) + z = x + (y + z)$.

Proof True $z = 1$, since then LHS $= S(x + y)$, RHS $= x + S(y)$.

Suppose true for z, prove $(x + y) + S(z) = x + (y + S(z))$

LHS $= [(x + y) + z] + 1$, inductive hyp. and defn. $S(z)$

$= [x + \overline{y + z}] + 1$ ind. hyp.

$= S(x + \overline{y + z})$ defn.

$= x + S(y + z)$ defn.

$= x + (y + S(z))$ defn.

Thus true all z.

Theorem $x + y = y + x$.

Proof First prove $x + 1 = 1 + x$, by induction on x

Then prove $x + y = y + x$, all x, by induction on y

Definition $x.1 = x$

$x.S(y) = x.y + x$

Exercise 14

14.1. Using the Peano postulates prove that $yx + zx = (y + z)x$ and prove $xy = yx$

14.2. If rational numbers are defined as ordered pairs of integers $p = (x,y)$, determine the rules for equality, addition, and multiplication, and prove that $p + q = q + p$. Identify the elements 0 and 1 such that $p + 0 = p$, and $p.1 = p$. and the elements ^{-}p (s.t. $p + {}^{-}p = 0$) and p^{-1} ($p \neq 0$, s.t. $p.p^{-1} = 1$). (Assume all properties of integers).

14.3. Assuming any properties of real numbers, and defining complex numbers as ordered pairs of real numbers $z = (x,y)$, prove that addition and multiplication of complex numbers are each commutative, that multiplication is distributive over addition, and that every element $z \neq (0,0)$ has an inverse z^{-1} s.t. $zz^{-1} = 1$.

(e) Hilberts' Programme

We mentioned in Appendix I the interesting suggestion that it might be possible to prove the consistency of mathematics by an axiomatic approach. Hilbert attempted to do this. (For a fuller account of this large undertaking, and its outcome, see Nagel and Newman (1971); the version which follows is brief and necessarily over-simplified). Since we can construct a model of Lobachevsky's non-Euclidean geometry within ordinary Euclidean geometry (see Courant and Robbins, 1941, p.221), non-Euclidean geometry is consistent if Euclidean geometry is. (For a contradiction within the one would imply a contradiction within the other). In the same way Euclidean geometry ca[illegible]d (by Cartesian coordinate geometry) within the real numbers and so by a chain of reasoning, within the natural numbers (p. 60) . Each of these models provides a relative consistency proof; the question of whether the geometry of the physical world is Euclidean or non-Euclidean is a different one, to be settled by experiment. (Both describe equally accurately geometry as it applies to everyday life; it is possible that for phenomena on a large scale, as in astronomical studies, a non-Euclidean version is more appropriate). It might still be the case that both geometries are inconsistent, and neither accurately describes the physical world. Nor dare we assert that, say, the arithmetic of natural numbers is self-evidently true, and hence consistent; the Russell set paradox illustrates the dangers here (see above). Part of the problem is that models for the natural

numbers have an infinite number of elements, so that we cannot, as in a finite case, examine the whole model to verify the axioms and check for inconsistencies.

Hilbert sought a proof of absolute consistency based on two principles. Mathematics was, for this purpose, to be completely formalised - reduced to a system of meaningless marks (which were nevertheless capable of bearing an interpretation in more familiar terms), manipulated by certain specified rules. In particular all operations with formulae had to be 'finite' in character. A proof is a sequence of formulae each of which is either an axiom or deducible from some previous formula by one of the specified rules.

(f) Propositional calculus

As an example of this type of proof, we prove a theorem of the 'calculus of propositions'. The symbol $\vee$ which occurs here may be interpreted as 'or' (though as we have said the proof does not involve meaning at all), i.e. $P \vee Q$ may be thought of as "P or Q (or both)". P,Q etc. may be interpreted as statements which are either true or false. We shall presently† consider the use of truth tables; each proposition P,Q . . . may be assigned a symbol (T or F, which we may think of as 'true' and 'false') and the statement P 'or' Q is then defined to have the "truth value" shown in the table. The tables for implication ($\Rightarrow$) and conjunction ($\&$, "and") are also given for comparison; it will be seen that the interpretations of T and F agree with previous notions of $\Rightarrow$ and $\&$.

P	Q	PvQ	P ⇒ Q	P & Q	(∼P)vQ
T	T	T	T	T	T
T	F	T	F	F	F
F	T	T	T	F	T
F	F	F	T	F	T

We note that the definition of $P \Rightarrow Q$ agrees with that of $(\sim P) \vee Q$.

† p102.

The axioms of the Propositional calculus are:-

1) $P \vee P \Rightarrow P$

2) $P \Rightarrow P \vee Q$

3) $P \vee Q \Rightarrow Q \vee P$

4) $P \Rightarrow Q .\Rightarrow. (R \vee P) \Rightarrow (R \vee Q)$ (where $P \Rightarrow Q$ means $(\sim P) \vee Q$).

(The full stop ⊙ identifies the 'major' implication sign, obviating brackets)

The permitted rules of inference are :-

1) Substitution (i.e. as in ordinary algebra the same expression may be substituted throughout for a proposition such as P,Q ...).

2) Detachment (sometimes called "modus ponens")

Given $P \Rightarrow Q$

and 'P is true'

we may write 'Q is true'.

Theorem $P \vee \sim P$ (Law of the Excluded Middle - interpreted as P is either true or false, but note that we deduce this from the axioms alone.

Proof $P \Rightarrow Q .\Rightarrow. (\sim R \Rightarrow P) \Rightarrow (\sim R \vee Q)$. ∼R for R in (4)

5) $P \Rightarrow Q .\Rightarrow. (R \Rightarrow P) \Rightarrow (R \Rightarrow Q)$ rewriting

(Thus we have a new 'chain' rule of inference. $R \Rightarrow P$, $P \Rightarrow Q$ / $R \Rightarrow Q$),

6) $R \Rightarrow R \vee R$ R for P and Q in 2

$R \vee R \Rightarrow R .\Rightarrow. (R \Rightarrow R \vee R) \Rightarrow (R \Rightarrow R)$ RvR for P, R for Q in 5.

$R \vee R \Rightarrow R$ R for P in 1

$R \Rightarrow (R \vee R) .\Rightarrow. (R \Rightarrow R)$ detachment.

7) $R \Rightarrow R$ detachment and 6.

8) $\sim R \vee R$ rewriting 7

$\sim R \vee R \Rightarrow R \vee \sim R$ ∼R for P, R for Q in 3.

$R \vee \sim R$ detachment and 8.

It may also be shown that $P \Rightarrow (\sim P \Rightarrow Q)$

and $(P \wedge \sim P) \Rightarrow Q$.

are theorems.

The second of these may be interpreted as "if a proposition and its negation are both provable then any formula is provable". Hilbert used this to prove consistency - it is only necessary to exhibit one formula which is not provable from the axioms, and then the system cannot be inconsistent.

Such a formula is PvQ (See below).

(g) Hilbert's consistency proof for the propositional calculus.

PvQ is not provable (outline of proof).

1. Definition If when the symbols T, F are assigned to the propositions P,Q, ... in all possible ways, a formula always takes the value T, then the formula is a tautology (example Pv (~ P) is a tautology).
2. Every axiom is a tautology.
3. The rules of inference transmit the tautological property - i.e. every provable theorem is a tautology, i.e. any formula which is not a tautology is not provable.
4. PvQ is not a tautology.

It can also be shown, conversely, that every tautology is provable, so that we have a simple means of determining whether a formula is or is not a theorem. :- the theorems are those, and only those, statements which are tautologies.

Thus the propositional calculus is consistent and complete (p.57).

(h) Gödel's work

Encouraged by this success, Hilbert and his collaborators then extended their work and were successful in proving that the Peano axioms alone are consistent, and remain so when the definition of addition is added. Hopes of ultimate success were dashed, however, by the work of Gödel who proved that :-

(1). If arithmetic is consistent, it is incomplete; i.e. there are statements of arithmetic which can neither be proved true nor proved false within the system.

(2). It is not possible to prove, within the system of arithmetic, that arithmetic is consistent.

(Here 'arithmetic' means the Peano axioms with definitions for + and x).

Gödel further showed that the situation was irretrievable, for if in (1) further axioms were adjoined - so that the 'undecidable' statements or their negations become axioms — other statements could always be found, which would be capable neither of proof nor disproof.

Similar results to those of Gödel have been found in the theory of algorithms. We may ask the question - "Is there a systematic method for finding all the real roots of a polynomial equation

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0$$

where n is an arbitrary positive integer, to any desired degree of accuracy?" The answer is 'yes'; texts on the theory of equations give such methods. In a celebrated lecture in 1900 Hilbert asked - "Is there a systematic method of solving all possible Diophantine equations?" (i.e. equations whose solutions are integers, such as $x^2 + y^2 = z^2$, $5x + 3y = 117$, and $x^4 + y^4 = z^4$; see Appendix IIIC, p.91).

The answer has recently been shown to be "no". (See Stewart (1975) p.296).

There is no general method which will tell us whether or not a given Diophantine equation has solutions, and if so, what they are. These impossibility proofs are like those in Chapter 6 - they assert that it is logically impossible that certain general algorithms should exist, which seems to guarantee that mathematics will continue to provide unsolved problems!

(A readable introduction to the theory of algorithms is given in Trakhtenbrot, 1963).

APPENDIX III

D. "Twenty Questions" - A selection of counter examples

Some of the following (marked *) are converses of true theorems, but are themselves false. Others are plausible conjectures, based on 'continuing a pattern' or on 'common sense', but nevertheless false.

On numbers

(1)* If n is prime then $2^n - 1$ is prime (Mersenne's numbers).
True for n = 2, 3, 5, 7, 11, . . False for n = 67, 257...(Reid, (1968), p88).†

(2)* If n is prime, then u_n, the nth Fibonacci number, is prime.
(See Exercise 17.4, p 83 and p 120).
False for n = 19 ; $u_{19} = 4181 = 37.113$

(3) In the factorisation $x^n - 1 = (x - 1)f(x)$, f(x) is a product of polynominals all of whose coefficients are +1 or -1. False, n = 105. (Sominskii, (1963) p5).

On matrices

(4)* If $A^2 = A$ then A = I or 0 $\quad A = \begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix}$

(5)* If AB = 0 then A = 0 or B = 0 $\quad A = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

(6) $A^2 - B^2 \equiv (A + B)(A - B)$

On limits and series

(7)* If $a_n < b_n$ (for $n > N$), $\lim_{n\to\infty} a_n < \lim_{n\to\infty} b_n$ $\quad (a_n = \frac{1}{2n},\ b_n = \frac{1}{n})$

(8)* If $u_n \to 0$, $\sum u_n$ is convergent $\quad (u_n = \frac{1}{n})$

(9) If an infinite series is rearranged its sum is unchanged.

$S = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} \ldots$

$\sigma = 1 - \frac{1}{2} - \frac{1}{4} + \frac{1}{3} - \frac{1}{6} - \frac{1}{8} \ldots$

$(\sigma = \frac{1}{2} S = \frac{1}{2} \log_e 2)$.

(and see p. 54)

† (see footnote p.34 and Sierpinski (1964), p.89)

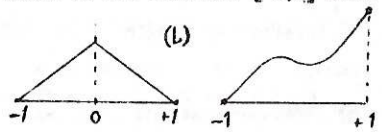
(10)* If an infinite series converges when some of its terms are bracketed together, then it still converges when the brackets are removed.
(1 - 1) + (1 - 1) + (1 - 1).....

(11) If $\sum u_n(x)$ is convergent with sum S(x) and $u_n(x)$ is continuous for each n } then S(x) is continuous.

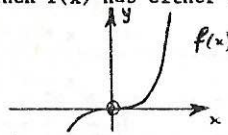
$u_n(x) = \frac{x^2}{(1+x^2)^{n-1}}$ $\quad S(x) = 1 + x^2,\ x \neq 0$; $S(0) = 0$ }

Calculus and Analysis

(12) If f(x) attains its greatest value in the interval [-1,1] when x = c then $f'(c) = 0$. (a) (b)

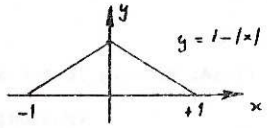


(13) If $f'(a) = 0$ then f(x) has either a maximum or a minimum value at a



(14)* A function which is continuous is differentiable.

(a)



(b) $f(x) = x \sin \frac{1}{x},\ x \neq 0$; $f(0) = 0$ } $\quad f'(0)$ does not exist

(15) If $f'(x)$ exists for all x in [0,1], then $f'(x)$ is continuous.

$f(x) = x^2 \sin \frac{1}{x},\ x \neq 0$; $f(0) = 0$ } $\quad f'(x) = 2x \cdot \sin \frac{1}{x} - \cos \frac{1}{x}$ $(x \neq 0)$; $f'(0) = 0$ }

(16) Every function has a power series expansion.
$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$.
$y = \log x$ has no power series expansion in any interval (a,b)

(17) Two sets of points A,B on the interval [0,1] have the property that between any two members of A there is a member of B, and between any two members of B there is a member of A. Then there are as many points in A as in B (i.e. $\exists$ a 1-1 correspondence between A and B).
False A = rationals, B = irrationals.

(18) It is impossible to set up a 1-1 correspondence between A and B where B is a proper subset of A. ("The whole is greater than the part", Euclid). False $A = \{1, 2, 3. \ . \ . \ .\}$ $B = \{2, 4, 6, 8, \ . \ . \ .\}$ (†)

(19) If each of the infinite number of rational points lying in the interval (0,1) is entirely enclosed within an interval, the total length of the enclosing intervals must be at least 1. (False). Enclose the n^{th} rational point, in some enumeration, in an interval of length $\frac{\varepsilon}{2^n}$. Then the total length is

$\varepsilon(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ . \ . \ ) = \varepsilon$, and may be as small as we please.

(20) n equations in n unknowns have a unique solution.

(a) $x + y = 7$
$x + y = 10$
$z = 3$

(b) $x + y = 7$
$x + z = 10$
$2x + y + z = 17$

(†) Galileo, G. Dialogue concerning Two New Sciences. (reprint 1954)

APPENDIX III

E. Some miscellaneous useful methods of obtaining proofs

1. Transformation of a problem into an equivalent problem

Examples

(a) How many <u>different</u> products arise when we expand $(a + b + c + d)^8$? (Some possibilities are a^8, a^7b, a^7c etc. We are <u>not</u> concerned with their coefficients). If we write the typical product $a^3b^2cd^2$ as aaa/bb/c/dd we can see this is equivalent to an arrangement of 8 stars and 3 strokes ***/**/*/**. (In the same way ***//*****/ corresponds to a^3c^5).

But the number of ways of arranging 8 stars and 3 strokes in order is easily seen to be ${}_{11}C_3$ (in which 3 positions, of the 11, are strokes to be placed?) Thus the number of different products is ${}_{11}C_3 = 135$.

(b) How long does it take to collect a set of picture cards? (e.g. from tea packets - assume random distribution).

Suppose we have collected 17 out of a set of 20. Probability of success on next occasion is $\frac{3}{20}$, so the problem is equivalent to drawing (with replacement) one red marble from an urn† containing 17 black and 3 red marbles. The expected waiting time for 'success' is

$1.\frac{3}{20} + 2.\frac{17}{20}\cdot\frac{3}{20} + 3.\left(\frac{17}{20}\right)^2\cdot\frac{3}{20} + \ . \ . \ . = \frac{20}{3} = 6\frac{2}{3}$ (See p.106 Exercise 20.2)

Hence the total waiting time (to collect a complete set of 20) is

$\frac{20}{20} + \frac{20}{19} + \ . \ . \ . + \frac{20}{3} + \frac{20}{2} + \frac{20}{1} = 20\left(\ + \frac{1}{2} + \frac{1}{3} + \ + \frac{1}{20}\right) = 69.95$

i.e. we need, on average 70 packets of tea to get a complete set of cards.

---

† The complaint is sometimes heard that "probability theory is all about drawing coloured balls from urns - and not about real life". Many 'real life' situations can be 'modelled' by a corresponding urn problem.

The method of mathematical induction is most obviously useful in dealing with problems involving integers. However, as the example below shows, it may be applied in other situations, where the integer variable to be used as the basis of the induction is not immediately apparent. (See also example (b) p. 81 and Ex. 16,18, p. 80).

Example

(Sominskii 1961, page 22) If a finite sequence of operations consisting of m operations chosen from +, -, x, - are performed on the complex numbers $z_1, z_2 \ldots z_n$, giving the result u, the same sequence of operations performed on their complex conjugates $\bar{z}_1, \bar{z}_2, \ldots \bar{z}_n$ will give the result $\bar{u}$, the complex conjugate of u. (The proof is by induction on m, the number of operations in the sequence.)

6. Impossibility and existence proofs

(a) To prove that $\sqrt{3}$ is irrational

Let k be the least integer n such that $n(\sqrt{3})$ is an integer.

Consider the integer $(2 - \sqrt{3})k$, (which is $< k$).

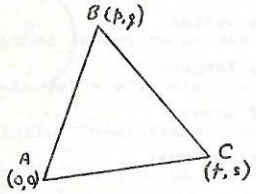
Then $(2 - \sqrt{3})k.\sqrt{3} = 2k.\sqrt{3} - 3k$ is an integer and so

$(2 - \sqrt{3})k$ is a possible value of n for which $n(\sqrt{3})$ is integral.

(contradiction)

(Adapted from Estermann, (1975), where a proof of the irrationality of $\sqrt{2}$ is given. A collection of such proofs may be found in The Mathematics Teacher (U.S.A.), Jan. 1971).

(b) A, B, C are 3 points in the plane with integer co-ordinates. Show that the Δ ABC cannot be equilateral.



Clearly we can take one vertex as (0,0).

Then $p^2 + q^2 = r^2 + s^2$

$= (p-r)^2 + (q-s)^2$

$= p^2 + q^2 + r^2 + s^2 - (2pr + 2qs)$.

i.e. $p^2 + q^2 = r^2 + s^2 = 2pr + 2qs$.

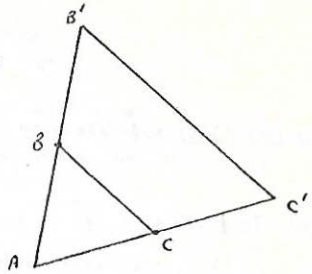
Thus p,q are both odd or both even; similarly for r,s.

If p,q both even $\Rightarrow r^2 + s^2 = M(4) \Rightarrow$ r,s not both odd.

Thus p,q,r,s all even and $\exists$ a smaller Δ (which leads to a contradiction).

If p,q,r,s are all odd, then pr + qs is even and $p^2 + q^2$ is M(4)

(impossible).

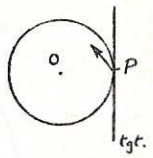


This method uses ideas of parity and of infinite descent. Alternatively, assuming the irrationality of $\sqrt{3}$, (above) let B′ be (2p,2q) and C′ (2r,2s). Then $\triangle$ ACB′ is right angled and $\frac{B'C}{AC} = \frac{\sqrt{3}}{1} = \frac{2q-s}{r}$ by similar $\triangle$'s.

But this implies $\sqrt{3}$ is rational (contradiction).

(c) Brouwer's fixed point theorem (See Courant and Robbins (1941), p. 251). A continuous transformation may be thought of as one in which points which are 'close together' initially are still 'close' after the transformation - as when we stretch a piece of rubber without cutting or tearing it. Brouwer proved that if a circular disc is continuously transformed into itself, at least one point of it must remain fixed.

Suppose no point remains fixed. Every point P on the circumference, C, must move to a (nearby) point of the disc. We show the direction of movement by a vector arrow, which must lie on the same side of the tangent line as does the centre of the disc, O. As P moves around the circumference of the disc, this vector must rotate through an integral number, i, of complete turns. Moreover, since the vector cannot cross, or coincide with, the tangent line, we must have i = 1. Now consider a slightly smaller circle, lying inside C. By continuity the vector for this circle must rotate through nearly (and so, exactly) the same angle (since i must be integral). Continuing to shrink the inner circle we arrive at a contradiction; on a very small circle the transformation vector must point in almost the same direction throughout (by continuity), so that i must be zero.



(Topological fixed point theorems such as these may appear totally unrelated to practical matters - but in point of fact they do have important practical applications in proving the convergence of sequences used in iterative calculations).

Other proofs of impossibility

(d) Three famous problems of antiquity which interested Greek mathematicians were the duplication of the cube, the trisection of an angle, and 'squaring the circle'. All were to be accomplished by ruler and compasses constructions; the first involved doubling the volume of a cube by constructing a line $\sqrt[3]{2}$ times the length of the cube, the third constructing a square of area equal to that of a circle of given radius. All have subsequently been proved impossible - some details are given in Courant & Robbins, 1941, p.134.

(e) Another impossibility proof concerns the solution of algebraic equations in one variable, real or complex. Any quadratic equation can be written in the form $Ax^2 + Bx + C = 0$, with solution $x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$.

A method known as Cardan's method, though not discovered by him, enables one to solve a general cubic equation. (If the cubic equation, after a suitable linear transformation, is $x^3 + 3Hx + G = 0$, we write $x = u + v$, $-G = u^3 + v^3$, $-H = uv$ so that u^3, v^3 are the roots of $t^2 + Gt - H^3 = 0$, whence x can be found by extracting square roots and cube roots).

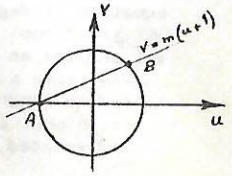
It might be expected that a similar reduction would be possible for an equation of degree 4 (solving in terms of fourth roots, etc.), which is so, and for an equation of degree 5 — which is not. As mathematicians failed to find a solution method, they began to suspect that no such method existed, and in due course it was proved by N.H. Abel that "the general equation of degree n is not solvable by radicals for $n \geq 5$". Far from closing-off an area of mathematics this discovery led to a

branch of group theory, known as Galois theory after its creator, which seeks to determine in what circumstances an equation is solvable by radicals. This was part of a wider movement in algebra, and in mathematics as a whole, away from methods of solving equations etc., and towards the study of underlying fundamental structure which is so characteristic of much of higher mathematics today.

(f) A famous, and as yet unsolved, problem is that known as Fermat's 'last' theorem. He stated, with a claim that he had a proof, that the equation $x^n + y^n = z^n$ has no solution with x,y,z natural numbers, for $n > 2$. (When $n = 2$ this is the well-known Pythagorean equation, $x^2 + y^2 = z^2$, with an infinity of solutions, including the even better-known triple (3,4,5)). Despite much effort, which has led to the development of substantial areas of mathematics, Fermat's conjecture has neither been proved nor disproved, although it is known to be true for $n \leq 25000$ (Selfridge & Pollock, Notices of the American Mathematical Society, 11, 1964, p.97).

We consider two cases:-

(i) $n = 2$ i.e. $x^2 + y^2 = z^2$. We show that $x = p^2 - q^2$, $y = 2pq$, $z = p^2 + q^2$ where p,q have no common factor, and just one of them is even, is a solution, and conversely that all solutions are of this form. (It is convenient to consider only the primitive triples, in which x,y,z have no common factor. This excludes the case p and q both odd). The theorem is immediately verifiable; for the converse we seek all rational solutions of $u^2 + v^2 = 1$ (a circle). The intersection of the line $v = m(u + 1)$ with this circle is the point P(-1,0), together with another point B, rational if and only if u and m are rational.



At A and B, $m^2(u + 1)^2 + u^2 - 1 = 0$

$\Rightarrow u = -1$ or $u = \frac{1 - m^2}{1 + m^2}$

Writing $m = \frac{q}{p}$, $u = \frac{x}{z}$ we have $\frac{x}{z} = \frac{p^2 - q^2}{p^2 + q^2}$ etc. as required.

Alternatively: It is clear that x odd, y odd is not possible, for then $z^2 \equiv 2$, mod 4.

Suppose y is even. $(z - x)(z + x) = y^2 = 4k^2$ and since $\left.\begin{matrix} z - x \\ z + x \end{matrix}\right\}$ have the same parity, they must be even. But $z - x$, $z + x$ can have no common factor > 2 (or else this would be a factor of z, of x, and so of y). Thus $z + x = 2p^2$, $z - x = 2q^2$, $\Rightarrow z = p^2 + q^2$, $x = p^2 - q^2$, $\Rightarrow y = 2pq$.

(ii) $n = 4$ i.e. $x^4 + y^4 = z^4$. We show this has no solution by showing that $x^4 + y^4 = z^2$ has no solution:-

Suppose the latter equation has a solution:

Then $x^2 = p^2 - q^2$, $y^2 = 2pq$, $z = p^2 + q^2$ } with p,q having no common factor and with one of them even, by (i) above. Clearly q must be even, since $x^2 \not\equiv 3$, mod 4.

Let $q = 2s$, $\Rightarrow y^2 = 4ps$ (which since p,s have no common factor) $\Rightarrow p = z_1^2$, and $s = t^2$.

Then $x^2 = (z_1^2)^2 - (2t^2)^2$ and so x, $2t^2$, z_1^2 are a Pythagorean triad:-

$z_1^2 = \ell^2 + m^2$

$x = \ell^2 - m^2$

$2t^2 = 2\ell m$

From $t^2 = \ell m$ we have $\ell = x_1^2$ and $m = y_1^2$ since ℓ,m have no common factor.

Now $z_1^2 = (x_1^2)^2 + (y_1^2)^2 = x_1^4 + y_1^4$ which is of the same form as the original equation,

but with $z = z_1^4 + 4t^4 > z_1^4 > z_1$ (since $z_1 > 1$).

We could now repeat the procedure and obtain a solution of $z_1^2 = x_1^4 + y_1^4$ with $z_2 < z_1$, and so on indefinitely. Thus by Fermat's 'method of infinite descent' we obtain a contradiction, as required.

(g) Finally we prove: e is irrational. (See Courant and Robbins (1941), p. 298)

Suppose $e = \frac{p}{q}$ for some natural numbers p,q.

Then $q!\,p$ is an integer. But $e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} \cdots + \frac{1}{q!} + \frac{1}{(q+1)!} + \ldots$

so that $q!\,p = M + \left(\frac{1}{q+1} + \frac{1}{(q+1)(q+2)} + \frac{1}{(q+1)(q+2)(q+3)} \ldots\right)$ where M is an integer

$= M + B$, say.

Now $0 < B < 1$, strictly, for $B < \frac{1}{q+1} + \frac{1}{(q+1)^2} + \frac{1}{(q+1)^3} \ldots = \frac{1}{q} < 1$

so that M + B cannot be an integer.

Further examples of existence proofs

(h) A sequence of n positive integers is given where n is odd. These are re-ordered, and the members of the second sequence are each subtracted from their counterparts in the first sequence. Then the product of the differences is even.

Proof. Evidently it is sufficient to show that one difference is even. Let the sequences be $u_1, u_2, u_3 \ldots u_n$ and $v_1, v_2, v_3 \ldots v_n$. If $(u_i - v_i) = 0$ for any i, the result follows. Since n is odd, the set $\{u_i\}$ must contain either a majority of odd elements or a majority of even elements, and in either case, for some i, $(u_i - v_i)$ is the difference of two odd elements (case 1) or of two even elements (case ii) — and so is even.

The proof is an example of the use of Dirichlets' pigeon-hole (U.S.: "mailbox") principle; "If m letters are placed in n boxes, $m > n$, then at least one box will contain 2 letters". Consider the 'majority' elements of $\{u_i\}$ - suppose these are odd. (A similar proof holds if these are even). There must be at least $\frac{n+1}{2}$ odd elements of $\{u_i\}$, and in the re-arrangement these cannot all be paired with the (at most $\frac{n-1}{2}$) other elements of $\{u_i\}$, so that at least 2 of them must be paired together.

Exercise 19.

19.1 Prove F_i, F_j have no common factor if $i \neq j$.† (Hint: express $(F_i - 1)$ in terms of $(F_j - 1)$, $i > j$). Hence show the number of primes is infinite.

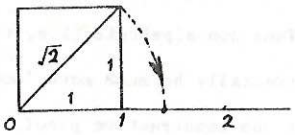
19.2 Show that there is an infinite number of primes of the form 4k + 3. (Hint: show that a composite number of the form 4k + 3 must have at least one factor of the same form; then consider $4.7.11.19 \ldots p_n + 3$, where p_n is the 'last' 4k + 3 prime).

19.3 Show that it is possible to find a set of 100 consecutive numbers, none of which is prime.

(i) Transcendental numbers

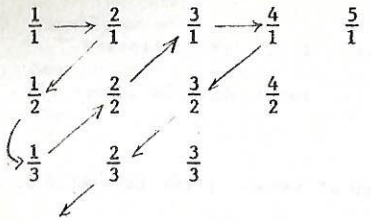
We have already shown that not all numbers are rational (e.g. $\sqrt{2}$ is irrational). This is surprising in view of the fact that between any two rational numbers there is an infinity of other rationals. (It is enough to find one; then we can repeat indefinitely. Either $\frac{a+c}{b+d}$ or $\frac{1}{2}\left(\frac{a}{b} + \frac{c}{d}\right)$ will serve).

So if we examine the segment (1,2) of the number line, it is 'thickly populated' with points representing rational numbers - infinitely many in number, as close together as we please - and yet $\sqrt{2}$ does not coincide with any of them.



We can show that the rational numbers are countable - that is, we can make a list of rational numbers in which every rational number will appear at some defined place. (We call this 'setting up a 1-1 correspondence' between the set of rationals and the set $\{1,2,3, \ldots\}$).

† (see p. 5).



Write down the rational numbers in order as indicated by the arrows, deleting those which have already been encountered:-

$$1 \quad 2 \quad \frac{1}{2} \quad \frac{1}{3} \quad \frac{2}{2} \quad 3 \quad \ldots$$

(It is easy to include the negative rationals - e.g. by inserting $-\frac{a}{b}$ immediately after $\frac{a}{b}$).

$\sqrt{2}$ can be expressed by an infinite decimal 1.414.....

It can be shown that every rational number can be represented by a repeating infinite decimal, and conversely. (See Courant and Robbins (1941), p67)

Though $\sqrt{2}$ is not rational, it is algebraic - that is it is the root of the algebraic equation $x^2 - 2 = 0$. However, there exist numbers which are not algebraic - they are not roots of algebraic equations. Such numbers are called transcendental; examples are the numbers e and π, though to prove these numbers transcendental is not easy (a discussion may be found in Klein (1939), Vol. I, pp. 237 ff).

Cantor was able to prove the existence of transcendental numbers. He first showed that the algebraic numbers are countable, and then that the real numbers, represented by all possible infinite decimal expressions, are not countable. Thus non-algebraic (i.e. transcendental) numbers must exist (and must, incidentally be much more 'numerous' than algebraic numbers!) This was a non-constructive proof. Liouville was the first to prove constructively that transcendental numbers exist, by showing that certain numbers are transcendental - for example

$\ell = 0.1100010\ldots01\ldots$

$= \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^6} + \frac{1}{10^{24}} \ldots$ where the indices are $1 = 1!$

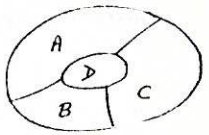
$2 = 2!$

$6 = 3! = 3 \times 2 \times 1$

$24 = 4! = 4 \times 3 \times 2 \times 1$

Further details are given in Courant & Robbins (1941), p104.

(j) The four-colour conjecture. A famous problem concerns colouring a plane map so that no two countries with a boundary in common are marked with the same colour.



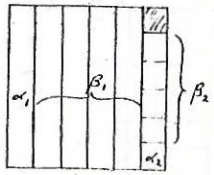
Any map can be coloured using 5 colours (See Courant & Robbins, (1941), p.246 and p.264). Four colours have been found adequate to colour every map so far encountered, and it is easy to produce one which cannot be coloured with only 3 colours.

So there remained a gap - 4 colours are necessary, and 5 colours are sufficient. Can we either find a map needing 5 colours, or prove that 4 colours are sufficient? It was conjectured that 4 colours are sufficient, and this was finally proved only very recently by an extensive enumeration of cases (using a computer to verify some of the details) - see Appel and Haken (1977).

Exercise 15

15.1. Demonstrate that $\frac{1}{6} + \left(\frac{1}{6}\right)^2 + \left(\frac{1}{6}\right)^3 + \ldots = \frac{1}{5}$

by dividing a unit square into 6 strips and proceeding as shown, with $\beta_i = 4\alpha_i$.

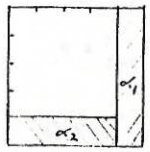


Draw a similar diagram for

$\frac{1}{3} + \left(\frac{1}{3}\right)^2 + \left(\frac{1}{3}\right)^3 + \ldots$

15.2. Demonstrate that $\frac{4}{5} + \left(\frac{4}{5}\right)^2 + \ldots = 4$

by 'cutting off one fifth' at each stage, starting with the unit square as shown. $\alpha_1 + \alpha_2 = \frac{1}{5} + \frac{1}{5}\left(\frac{4}{5}\right)$. The area remaining is a square, and the process can be repeated.



Draw a similar diagram for $\frac{2}{3} + \left(\frac{2}{3}\right)^2 + \ldots$

15.3. By considering the graph of $y = \frac{1}{x}$ show that $S_n = 1 + \frac{1}{2} + \ldots + \frac{1}{n} > \log_e (n+1)$

and that $S_n - \log_e(n+1)$ increases with n, but is always less than 1.

(This proves that $S_n - \log_e(n+1)$ tends to a limit γ where $\gamma \leq 1$).

Show Euler's constant γ satisfies $\frac{1}{2} < \gamma \leq 1$ and find γ as accurately as you can.

15.4. For $x > -1$, $(1 + x)^n \geq 1 + nx$, $\quad n = 1, 2, 3, \ldots$

Prove this by considering the graph of $y = (1 + x)^n$.

B. Proofs by Mathematical Induction

(a) If $u_{k+1} = 3u_k - 2u_{k-1}$, $k = 1, 2, 3 \ldots$

and $u_0 = 2$, $u_1 = 3$, prove that $u_n = 2^n + 1$

We need to verify that $u_0 = 2^0 + 1$, $u_1 = 2^1 + 1$. (Note there are two 'starting conditions'). Now assume P_k and P_{k-1} are true (i.e. that $u_k = 2^k + 1$ and $u_{k-1} = 2^{k-1} + 1$.

$u_{k+1} = 3(2^k + 1) - 2(2^{k-1} + 1) = (3 - 1)2^k + 1 = 2^{k+1} + 1$ i.e. P_{k+1} is true.

Thus we have P_k and $P_{k-1} \Rightarrow P_{k+1}$

P_0, P_1 are true

} so the result follows by M.I.

Exercise 16 (Easy) Prove the following results by Mathematical induction:-

16.1 $1 + 3 + 5 + \ldots + 2n-1 = n^2$

16.2 $1 + 2 + 3 + 4 \ldots + n + (n-1) + (n-2) + \ldots + 3 + 2 + 1 = n^2$

16.3 $2^n \geq n^2$ for $n \geq 4$.

16.4 $1^3 + 2^3 + 3^3 + \ldots + n^3 = \frac{n^2 \cdot (n+1)^2}{4}$

16.5 Adapt the proof of p37 above to prove $(1 + x)^n > nx$ for $n = 2, 3 \ldots$ $\begin{cases} x \neq 0 \\ x > -1 \end{cases}$

16.6 Find an expression for $(1 - \frac{1}{4})(1 - \frac{1}{9})(1 - \frac{1}{16}) \ldots \left(1 - \frac{1}{n^2}\right)$

and prove your result by M.I.

16.7 $\sum_1^n \frac{1}{r(r+1)} = \frac{n}{n+1}$

16.8 $3^{2n} - 1$ is a multiple of 8.

16.9 $2^n + 1$, $2^n - 1$ are divisible by 3 if n is respectively odd, even.

16.10 Let $u_{n+1} = u_n + u_{n-1}$ for $n \geq 2$, $u_1 = u_2 = 1$, (the Fibonacci sequence).

Then $u_n = \frac{1}{\sqrt{5}}\left\{\left(\frac{1 + \sqrt{5}}{2}\right)^n - \left(\frac{1 - \sqrt{5}}{2}\right)^n\right\}$.

16.11 $a + ar + ar^2 + \ldots ar^{n-1} = a\frac{(1 - r^n)}{1 - r}$ (Geometric series)

16.12 $(1 + x)^n = 1 + {}_nC_1 x + {}_nC_2 x^2 + \ldots + {}_nC_r x^r + \ldots + x^n$ (Binomial theorem)

16.13 $(\cos\theta + j \sin\theta)^n = \cos n\theta + j \sin n\theta$, $j^2 = -1$. (De Moivre's theorem)

16.14 $D^n(uv) = D^n(u).v + {}_nC_1 D^{n-1}(u)D(v) + \ldots$

$+ \ldots {}_nC_r D^{n-r}(u)D^r(v) + \ldots + uD^n(v)$ (Leibnitz' theorem)

16.15 If $I_n = \int_0^\infty x^n e^{-x}\,dx$, $n \geq 0$, prove $I_n = nI_{n-1}$ and that $I_n = n!$.

16.16 $\sum_1^n r(r + 1)(r + 2) = \frac{n(n + 1)(n + 2)(n + 3)}{4}$

16.17 $\sin x + \sin 2x + \sin 3x + \ldots + \sin nx = \frac{\sin \frac{n+1}{2}x}{\sin \frac{x}{2}} \cdot \frac{\sin nx}{2}$

16.18 Any map consisting of the regions defined by n (infinite) straight lines in a plane can be coloured using only 2 colours.

Examples of more difficult proofs by mathematical induction

Exercise 16.3 illustrates that we are sometimes required to prove a result for $n \geq n_0$ where n_0 is greater than 1, in which case the induction 'starting point' is P_{n_0}.

Exercise 16.10 and Example (a) above illustrate the use of P_k and P_{k-1} in proving P_k; in some proofs we assume P_n for $n \leq k$ and then prove P_{k+1}

Woodall (1975) stresses an alternative approach to induction, regarding the task as being to prove P_{k+1} using P_k, P_{k-1}, ... etc. if this is necessary.

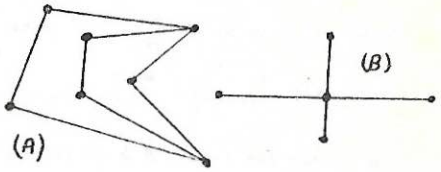
He remarks that the usual 'stepping up from P_k to P_{k+1}' approach does not always work. (See example (b) below). Both approaches are linked to a method used by Fermat - that of "infinite descent" - if there is an n s.t. P_n is not true, there must be some least integer k for which P_k is untrue. A contradiction is then arrived at either by proving P_k is true, or by finding $k' < k$ with $P_{k'}$ untrue.
(See pages 87, 91).

Example (c) illustrates what Hardy, Littlewood and Polya (1934) describe as "backward induction"; we have $P_k \Rightarrow P_{k-1}$ and P_k is true for an infinity of values of k, from which we conclude P_n is true for all n.

Sometimes a "double induction" involving two natural number variables is necessary (see (d), p.82, and also page 66.).

Examples (b) (Woodall, 1975)

A graph is a collection of arcs and vertices. The valency of a vertex is the number of arcs which meet there.



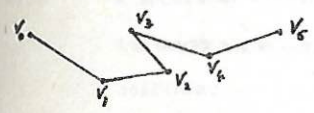
(In the illustration B has one vertex of valency 4, the rest of valency 1; A has all vertices with valency 3 or 2). A path is a succession of arcs with no repeated vertices.

Theorem. If every vertex has even valency, the arcs can be broken up into a number of circuits with no arcs in common.

Proof. By induction on the number of arcs n.

Let P_k mean "the theorem is true for every graph with k arcs". We assume $k > 0$ and try to prove P_k.

Find a longest path, through vertices say $V_0, V_1 \ldots V_m$. where $m > 0$ (since $k > 0$)



Since V_m has even valency it is joined to some other vertex and since the path is a longest path, this other vertex must be one of $V_0, V_1 \ldots V_{m-1}$ - say V_i

Then $V_i, V_{i+1}, V_{i+2} \ldots V_m$ is a circuit, the removal of which leaves a graph with fewer than k arcs, each vertex still having even valency.

By the induction hypothesis (P_n for $n < k$) the theorem is true for the reduced graph - and so for the original graph.

(Note: We have proved P_k by showing that it depends on P_n for some $n < k$. If we attempt to 'step up' from P_k to P_{k+1} by adding an arc, we obtain a graph which does not satisfy the condition of the theorem!).

(c) To show that the arithmetic mean A of n positive numbers $a_1, a_2 \ldots a_n$ is not less than their geometric mean G.

i.e. $\frac{a_1 + a_2 \ldots a_n}{n} = A \geqslant G = (a_1 a_2 \ldots a_n)^{\frac{1}{n}}$ c.f. Ch. 3, p 17, Ex. 7.4

When n = 2 we have $(a_1 + a_2)^2 = 4a_1 a_2 - (a_1 - a_2)^2 \geqslant 4a_1 a_2$, i.e. $\left(\frac{a_1 + a_2}{2}\right) \geqslant (a_1 a_2)^{\frac{1}{2}}$

Similarly $\frac{a_1 + a_2 + a_3 + a_4}{4} \geqslant \left(\frac{a_1 + a_2}{2} \cdot \frac{a_3 + a_4}{2}\right)^{\frac{1}{2}} \geqslant (a_1 a_2 a_3 a_4)^{\frac{1}{4}}$

and hence for $n = 2^m$, $A \geqslant G$ (or, we may use induction on m).

Thus P_{2^m} is true for any m.

Now suppose P_k is true and let $\alpha = \frac{a_1 + a_2 \ldots + a_{k-1}}{k - 1}$

Then for $a_1, a_2, \ldots, a_{k-1}, \alpha$ we have $\left(\frac{a_1 + a_2 + \ldots a_{k-1} + \alpha}{k}\right)^k = \alpha^k \geqslant a_1 a_2 \ldots a_{k-1} \alpha$

from which P_{k-1} follows

(d) Prove by induction that $n(n + 1) \ldots (n + r - 1)$ is a multiple of $r!$.

(The result is immediate if we note that $\frac{n(n + 1) \ldots (n + r - 1)}{r!} = {}_{n+r-1}C_r$,

which is a binominal coefficient - but it is of interest to try an inductive proof).

Let $f(r,n) = n(n + 1) \ldots (n + r - 1)$,

Suppose the theorem is true for all n when $r = s - 1$ } for some fixed s.
and that it is true for n = k when r = s. (P_{s-1}) }

We proceed first by induction on n, and then by induction on r (a double induction)

Case n = k + 1

$f(s,k + 1) - f(s,k) = (k + 1)(k + 2) \ldots (k + s) - k(k + 1) \ldots (k + s - 1)$

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

$= s.t\,(s - 1, k + 1) = s \times$ multiple $\left((s - 1)!\right)$, by induction hypothesis.

Thus the theorem is true when n = k + 1 and r = s

But when n = 1, $f(s,n) = s!$ so the result holds.

Hence the theorem is true for all n, when r = s, by induction on n.

i.e. $P_{s-1} \Rightarrow P_s$

But the theorem is true for all n when r = 1, (since n is divisible by 1).

Hence, by induction on r, it is true for all n and for all r.

Exercise 17 (Harder examples on induction)

17.1 Prove $u_n = \frac{1}{n} + \frac{1}{n+1} + \ldots + \frac{1}{2n+1} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} \ldots + \frac{1}{2n-1} = v_n$

(Hint. Prove $u_{n+1} - u_n = v_{n+1} - v_n$)

17.2 Use the identity $a^n + b^n = (a^{n-1} + b^{n-1})(a + b) - ab\,(a^{n-2} + b^{n-2})$

to prove that $\sqrt{3}\left[\sqrt{3 + 1}^{2m} - 1 + \sqrt{3 - 1}^{2m} - 1\right]$

is an integer divisible by 2^m.

17.3 If $n \geqslant 2$, $0 < a_i < 1$,

prove $(1 - a_1)(1 - a_2) \ldots (1 - a_n) > 1 - a_1 - a_2 - a_3 \ldots - a_n$.

17.4 If $u_{n+1} = u_n + u_{n-1}$ (all n), $u_1 = u_2 = 1$,

prove $u_{n+k} = u_{n-1} u_k + u_n u_{k+1}$

(Use P_k and P_{k-1} to prove P_{k+1})

17.5 Prove $A \geqslant G$ (see (c) above) as follows:-

Show by induction that for $a, b > 0$, $a \neq b$, $(n-1)a^n + b^n > na^{n-1} \cdot b$

Now substitute $a^n = \frac{a_1 + a_2 \ldots a_{n-1}}{n - 1}$ and $b^n = a_n$

17.6 A spherical cheese is sliced by n plane cuts, all passing close to its centre, but such that no four planes are concurrent, no three collinear, no lines of intersection parallel. If each circular cross section of the sphere is divided into R_{n-1} regions by the other (n-1) planes, prove by induction that $R_n = \frac{1}{2}(n^2 + n) + 1$. Hence prove the number of pieces into which the spherical cheese is divided by the n planes is $V_n = \frac{n^3 + 5n + 6}{6}$ (See exercise 2.4, p 6).

17.7 Prove (a) $\sum_1^n r^7 + \sum_1^n r^5 = \frac{1}{8} n^4 . (n+1)^4$

(b) $D^n (x^n \log x) = n! (\log x + 1 + \frac{1}{2} + \ldots + \frac{1}{n})$

(c) $n^7 - n$ is divisible by 7

17.8 If $D^n (e^{x^2/2}) = u_n e^{x^2/2}$, prove $u_n(x)$ is a polynominal of degree n in x which satisfies $u_{n+1} = u_n' + x u_n$. Show also that

$U_{n+1} = U_n + nU_{n-1}$ and hence find a differential equation satisfied by U_n, and the form of $U_n(x)$.

17.9 c.f. Exercise 2.3, p 6. A new point P_{n+1} is placed on the circumference of the circle and joined by chords to all the existing points $P_1 \ldots P_n$. (Suppose P_{n+1} lies on the arc $P_n P_1$).
Prove that

(a) the chord $P_{n+1}P_r$ meets $(n-r)(r-1)$ other chords, and produces $(n-r)(r-1) + 1$ new regions, $(n \geq 1)$, $r = 1$ to n,

(b) all the chords through P_{n+1} produce $\frac{n(n-1)(n-2)}{6} + n$ new regions,

(c) $R_n = \frac{n(n-1)(n-2)(n-3)}{24} + \frac{n(n-1)}{2} + 1$ (R_n = the number of regions).

Hint. Use the analogues of the result of Ex. 16.16, p 80.

17.10 Prove $a(n - a^{n-1}) \leq n - 1$, for all real a.

Exercise 18

These problems, although at first sight candidates for solution by mathematical induction, are NOT suitable for induction proofs. Solutions are given on page 122.

18.1 If $u_{n+1} = \frac{1}{2}\left(u_n + \frac{A^2}{u_n}\right)$ for $n = 1, 2, 3$ and $0 < A \leq u_1$ prove that $u_{n+1} \geq A$, and $u_{n+1} \leq u_n$. Hence show that $u_n \to a$ limit as $n \to \infty$.
Show that the limit is A. Prove also that $\frac{(u_n - A)^2}{2u_n} = (u_{n+1} - A)$,
(Induction is not centrally involved here - the proof is direct).

18.2 If x,y are positive real numbers $\frac{x^m y^n}{(x+y)^{m+n}} \leq \frac{m^m n^n}{(m+n)^{m+n}}$

(Hint: Use the result of (c) page 82, applied to m numbers equal to $\frac{x}{m}$, and n numbers equal to $\frac{y}{n}$).

18.3 Prove that $\frac{(2n)!}{n!\,(n+1)!}$ is an integer

Hints: (i) If p is a prime, $p \geq 2$, it occurs as a factor of n! with multiplicity $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$
where $[x]$ = greatest integer $\leq x$

(ii) Prove $[x] + \left[x + \frac{1}{p}\right] \leq [2x]$, $p \geq 2$
(Let $x = \lambda + \epsilon$, where $\lambda = [x]$, so $0 \leq \epsilon < 1$).

(iii) Let p be any prime factor of the denominator.....

Concluding notes

"Getting the induction started" - i.e. verifying P_1 (in most instances) or in general P_{n_0} - is often treated as a formality. That it is essential is shown by example (a). The remaining examples illustrate other fallacious 'proofs'.

(a) $\sum_1^n \frac{2}{3^r} > \sum_1^n \frac{3}{4^r}$ "Proof" Suppose P_k is true. The $(k+1)^{th}$ terms are $a_{k+1} = \frac{2}{3^{k+1}}$, $b_{k+1} = \frac{3}{4^{k+1}}$

and clearly for $k \geq 1$, $a_{k+1} > b_{k+1}$

"Hence the result is true by M.I."

(b) In any set of n natural numbers, all the numbers are equal.

"Proof" P_1 is obvious, so suppose P_k is true and consider the set $n_1, n_2, n_3 \ldots n_k, n_{k+1}$ Applying P_k we have $n_1 = n_2 = n_3 \ldots = n_k$ and applying P_k again we have $n_2 = n_3 = n_4 \ldots = n_{k+1}$, so that P_{k+1} follows.

(c) (Courant and Robbins 1941, p. 20).
Any two natural numbers are equal.

"Proof" Define max(a,b) as the greater of a and b, $a \neq b$, (and as a if $a = b$)
Let P_n be "If a,b are natural numbers with max (a,b) = n then a = b"
Evidently P_1 is true since if max (a,b) = 1, both a and b must be 1.
Suppose P_k is true, and let max (a,b) = k + 1
Then the numbers $\alpha = a - 1$, $\beta = b - 1$ are such that max $(\alpha, \beta) = k$, so that by P_k, $\alpha = \beta \Rightarrow a = b$. Hence P_{k+1} is true. (?).

The method of mathematical induction is most obviously useful in dealing with problems involving integers. However, as the example below shows, it may be applied in other situations, where the integer variable to be used as the basis of the induction is not immediately apparent. (See also example (b) p. 81 and Ex. 16, 18, p. 80).

Example

(Sominskii 1961, page 22) If a finite sequence of operations consisting of m operations chosen from +, −, x, ÷ are performed on the complex numbers $z_1, z_2 \ldots z_n$, giving the result u, the same sequence of operations performed on their complex conjugates $\bar{z}_1, \bar{z}_2, \ldots \bar{z}_n$ will give the result $\bar{u}$, the complex conjugate of u. (The proof is by induction on m, the number of operations in the sequence.)

APPENDIX III

I. Impossibility and existence proofs

(a) To prove that $\sqrt{3}$ is irrational

Let k be the least integer n such that $n(\sqrt{3})$ is an integer.

Consider the integer $(2 - \sqrt{3})k$, (which is $< k$).

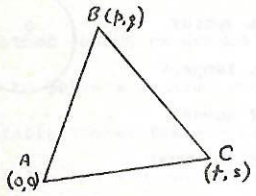
Then $(2 - \sqrt{3})k.\sqrt{3} = 2k.\sqrt{3} - 3k$ is an integer and so

$(2 - \sqrt{3})k$ is a possible value of n for which $n(\sqrt{3})$ is integral.

(contradiction)

(Adapted from Estermann, (1975), where a proof of the irrationality of $\sqrt{2}$ is given. A collection of such proofs may be found in The Mathematics Teacher (U.S.A.), Jan. 1971).

(b) A, B, C are 3 points in the plane with integer co-ordinates. Show that the Δ ABC cannot be equilateral.



Clearly we can take one vertex as (0,0).

Then $p^2 + q^2 = r^2 + s^2$

$= (p-r)^2 + (q-s)^2$

$= p^2 + q^2 + r^2 + s^2 - (2pr + 2qs)$.

i.e. $p^2 + q^2 = r^2 + s^2 = 2pr + 2qs$.

Thus p,q are both odd or both even; similarly for r,s.

If p,q both even $\Rightarrow r^2 + s^2 = M(4) \Rightarrow$ r,s not both odd.

Thus p,q,r,s all even and $\exists$ a smaller Δ (which leads to a contradiction).

If p,q,r,s are all odd, then pr + qs is even and $p^2 + q^2$ is M(4)

(impossible).

(18) It is impossible to set up a 1-1 correspondence between A and B where B is a proper subset of A. ("The whole is greater than the part", Euclid). False A = $\{1, 2, 3. \ldots\}$ B = $\{2, 4, 6, 8, \ldots\}$ (†)

(19) If each of the infinite number of rational points lying in the interval (0,1) is entirely enclosed within an interval, the total length of the enclosing intervals must be at least 1. (False). Enclose the n^{th} rational point, in some enumeration, in an interval of length $\frac{\varepsilon}{2^n}$. Then the total length is

$\varepsilon(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots) = \varepsilon$, and may be as small as we please.

(20) n equations in n unknowns have a unique solution.

(a) $x + y = 7$
$x + y = 10$
$z = 3$

(b) $x + y = 7$
$x + z = 10$
$2x + y + z = 17$

(†) Galileo, G. Dialogue concerning Two New Sciences. (reprint 1954)

E. Some miscellaneous useful methods of obtaining proofs

1. Transformation of a problem into an equivalent problem

Examples

(a) How many different products arise when we expand $(a + b + c + d)^8$? (Some possibilities are a^8, a^7b, a^7c etc. We are not concerned with their coefficients). If we write the typical product $a^3b^2cd^2$ as aaa/bb/c/dd we can see this is equivalent to an arrangement of 8 stars and 3 strokes ***/**/*/**. (In the same way ***//*****/ corresponds to a^3c^5).

But the number of ways of arranging 8 stars and 3 strokes in order is easily seen to be $_{11}C_3$ (in which 3 positions, of the 11, are strokes to be placed?) Thus the number of different products is $_{11}C_3 = 135$.

(b) How long does it take to collect a set of picture cards? (e.g. from tea packets - assume random distribution).

Suppose we have collected 17 out of a set of 20. Probability of success on next occasion is $\frac{3}{20}$, so the problem is equivalent to drawing (with replacement) one red marble from an urn† containing 17 black and 3 red marbles. The expected waiting time for 'success' is

$1.\frac{3}{20} + 2.\frac{17}{20}\cdot\frac{3}{20} + 3.\left(\frac{17}{20}\right)^2\cdot\frac{3}{20} + \ldots = \frac{20}{3} = 6\frac{2}{3}$ (See p.106 Exercise 20.2)

Hence the total waiting time (to collect a complete set of 20) is

$\frac{20}{20} + \frac{20}{19} + \ldots + \frac{20}{3} + \frac{20}{2} + \frac{20}{1} = 20\left(\ + \frac{1}{2} + \frac{1}{3} + \ + \frac{1}{20}\right) = 69.95$

i.e. we need, on average 70 packets of tea to get a complete set of cards.

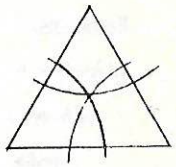
---

† The complaint is sometimes heard that "probability theory is all about drawing coloured balls from urns - and not about real life". Many 'real life' situations can be 'modelled' by a corresponding urn problem.

2. The pigeonhole principle

This has been referred to in Appendix III C,(h), p92. Here is a simple geometrical example.

(c) Show that in an equilateral triangular region (of side 1) it is impossible to place 4 points so that the distance between any two points is greater than $\frac{1}{\sqrt{3}}$.



Proof. If arcs, radius $\frac{1}{\sqrt{3}}$ and centres at the three three vertices, are drawn as shown, three partially overlapping regions are obtained. If 2 points are in the same region, their distance apart $\leq \frac{1}{\sqrt{3}}$. But if 4 points are placed in 3 regions, at least 2 points must be in the same region.

Further examples are given in Walker (1977) and Avital and Hansen (1976) - see Exercise 20.3.

3. Series

Useful methods here include the integration or differentiation of series with known sum (see Exercise 20.2), and the method of differences, in which each term u_n is expressed as a difference:-

$u_n = v_n - v_{n-1}$ Then $\sum_{k=1}^{n} u_k = (v_n - v_{n-1}) + (v_{n-1} - v_{n-2}) + \ldots + (v_2 - v_1)$

$= v_n - v_1$

(d) Example $\sum_{1}^{n} r(r+1) = \sum_{1}^{n} \frac{1}{3}\{(r)(r+1)(r+2) - (r-1)(r)(r+1)\}$

$= \frac{1}{3} n(n+1)(n+2)$

This result may also be proved by Mathematical Induction. There is an obvious analogy with $\int_0^m t^2 dt = \frac{m^3}{3}$)

Note also that if two sequences have the same starting values and obey the same recurrence relation, they are identical. (See Exercise 20.8, p107, and Appendix F, p111.).

4. If $a \geqslant b$ and $b \geqslant a$, then $a = b$.

This is a useful way of proving two numbers equal, two sets identical, etc.

(e) Examples

(i) (A 'Fundamental Theorem' of Linear Algebra)

Let U, V be vector spaces and let $f : U \to V$ be a linear map, with kernel ker f, defined by $k \in \ker f \Leftrightarrow f(k) = 0$ (see pp. 41, 61)

Then if $f(a) = b$, $f^{-1}(b) = a + \ker f$.

Proof

Let S be the set $f^{-1}(b)$.	Let $s \in a + \ker f$.
If $s \in S$ then $f(s) = b = f(a)$	then $s = a + k$, $k \in \ker f$
$\therefore f(s - a) = f(s) - f(a) = 0$	$f(s) = f(a) + f(k)$
so that $(s - a) \in \ker f$	$f(s) = f(a) = b$, since $f(k) = 0$
i.e. $s \in a + \ker f$	i.e. $s \in S$
$\therefore S \leqslant a + \ker f$	$\therefore a + \ker f \leqslant S$

Hence $a + \ker f = S$

As an application, consider $\frac{d^2y}{du^2} + 4y = 5e^x$.

$D^2 + 4 : C^2[a,b] \to C[a,b]$ This is a linear map between the two spaces of functions.

$\ker = \langle \sin 2x, \cos 2x \rangle$ (i.e. "A sin 2x + B cos 2x is the general solution of $(D^2 + 4)y = 0$", the complementary function).

A particular solution is e^x.

The general solution is $y = e^x + A \sin 2x + B \cos 2x$.

(ii) Rolle's theorem states:- If f is a continuous function on $[a,b]$, and differentiable in (a,b), and $f(a) = f(b)$ then $\exists$ c, $a < c < b$, s.t. $f'(c) = 0$. In the proof, we take c as an extremum of f and show $f'(c) \geqslant 0$, $f'(c) \leqslant 0$, and deduce that $f'(c) = 0$.

5. Exhaustion

This method (not a state of mind!) has been mentioned on p.32.

It is of limited use, and restricted to situations in which only a finite number of possibilities need be examined. As another simple example:-

(f) $n^3 - n$ is a multiple of 3 for all n.

In arithmetic mod 3, the only numbers are 0,1,2.

So we need only check that $0^3 \equiv 0 \pmod 3$

$1^3 \equiv 1 \pmod 3$

$2^3 \equiv 2 \pmod 3$

(equivalent to considering the three cases: n = 3k, 3k + 1, 3k + 2).

Note. Alternative proofs: mathematical induction; or

$n^3 - n = (n-1)n(n+1)$ and 3 consecutive numbers have factors 2 and 3.

Truth tables give rise to a form of proof by exhaustion.

e.g. to prove $(P \Rightarrow Q)\ \&\ (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$

we draw up the table:-

P	Q	R	P ⇒ Q	Q ⇒ R	LHS (P ⇒ Q) & (Q ⇒ R)	RHS P ⇒ R	LHS ⇒ RHS
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

Note. Compare with p. 69 . Here we do not prove the result by axiomatic methods, but by assigning meanings (T = true, F = false). The formula is a tautology - 'true' whatever the truth values assigned to P,Q,R by examining all 8 possible cases (though, as observed on p. 70 , it can be shown that every tautology is provable from the axioms).

6. Symmetry, parity, dimension

In some ways more useful as checks, these ideas can sometimes lead to proofs:-

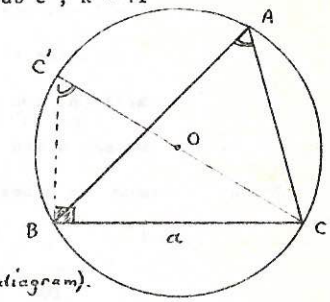
(g) Factorise $\begin{vmatrix} a & b & c \\ a^2 & b^2 & c^2 \\ a^3 & b^3 & c^3 \end{vmatrix}$

$\Delta = 0$ if $a = 0$ and if $a = b$

By symmetry $E = abc\,(a-b)(b-c)(c-a)$ is a factor

Since the degree is 6, $\Delta = kE$ and by coefficient of ab^2c^3, $k = +1$

(h) The diagram shows $\frac{BC}{CC} = \frac{a}{2R} = \sin A$



$OC = R$

i.e. $\frac{a}{\sin A} = 2R$

It follows that $\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C}$

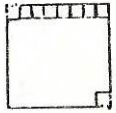
(The obtuse-angled case requires an alternative diagram).

(i) Problem: Three tumblers are placed upside down on a table. A 'move' consists of inverting any two tumblers. Is it possible, by a sequence of moves, to end with all three tumblers right way up?

Let N be the number of tumblers upside down.

(Initially N = 3). Clearly, inverting two tumblers changes N by -2 (as Ⓐ) or by 0 (as Ⓑ) or by +2 (e.g. Ⓐ reversed). Thus N must always be odd - and so can never be zero.

(j) Problem: The two opposite corner squares of an 8 x 8 chessboard are removed. Is it possible to cover the remaining squares with dominoes, each domino covering 2 squares?



No: for each domino must cover 1 white and 1 black square. But there are either 30 W and 32 B or 32 W and 30 B squares to be covered, so that eventually 2 squares of the same colour must be left.

Similar arguments can be used to investigate possible final positions in Solitaire. See also the Königsberg bridge problem p. 42.

(k) (Trivially) The surface area of a sphere cannot be $\frac{4}{3}\pi r^3$, since this has the dimensions of a volume.

The method of 'dimensional analysis' extends this checking principle into a tool of discovery. (See S.M.P. Advanced Mathematics, Book IV). As an example, suppose we are seeking a relationship between the frequency of vibration of a stretched string (ν) and other quantities such as its length (ℓ), its density (ρ), cross sectional area (A) and tension (F).

We may write $\nu = k\,\ell^p \rho^q A^r F^s$ where k is a dimensionless constant, and the other quantities have dimensions

$$[\nu] = \frac{1}{T} \qquad [A] = L^2$$
$$[\ell] = L \qquad [F] = MLT^{-2}$$
$$[\rho] = ML^{-3}$$

Now, equating indices we obtain:-

T) $-1 = -2s \Rightarrow s = \frac{1}{2}$

M) $0 = q + s \Rightarrow q = -\frac{1}{2}$

L) $0 = p - 3q + 2r + s \Rightarrow p + 2r = -2$

} so $\nu = \frac{kA^r}{\ell^{2r+2}}\sqrt{\frac{F}{\rho}}$

If we now use the fact that ν is proportional to $\frac{1}{\ell}$ (halving the length doubles the frequency), we have

$2r + 2 = 1$, $r = -\frac{1}{2}$, and $\nu = k.\frac{1}{\ell}\sqrt{\frac{F}{A\rho}}$

7. Assumptions of linearity, convergence, monotone functions, etc.

("try the simplest thing first" - Polya).

e.g.

(i) to prove $f > g$, for $x > 0$, prove $f(0) = g(0)$ and $f'(x) > g'(x)$ } †

(ℓ) Thus (assuming $D(\sin x) = \cos x$, $D(\cos x) = \sin x$), in $0 < x < \frac{\pi}{2}$

$1 > \cos x$

$\Rightarrow x > \sin x$ since $0 = \sin 0$

$\Rightarrow 1 - \frac{x^2}{2} < \cos x$ and $D(\sin x) = \cos x$

$\Rightarrow x - \frac{x^3}{6} < \sin x$

† This amounts to assuming that $\frac{d}{dx}(f-g) > 0$. See also p. 78 (Ex. 15.4) and p. 121 (Ex. 17.10).

(ii) Assume a function can be expanded as a power-series, which can be rearranged, multiplied or differentiated term by term. (See Ex. 20.2, 20.6, p106).

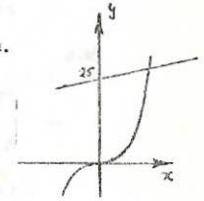
(m) Newton found a series for $y = \sin^{-1} x$ by 'inverting' that for sin x as follows:-

$y = \sin^{-1} x \Leftrightarrow \sin y = x = y - \frac{y^3}{6} + \frac{y^5}{120} \ldots$

$\therefore y = x + \frac{y^3}{6} - \frac{y^5}{120} \ldots = x + \frac{\left(x + \frac{y^3}{6}\right)^3}{6} - \frac{\left(x + \frac{y^3}{6}\right)^5}{120}$ (using $x + \frac{y^3}{6}$ as an approximation for y)

$= x + \frac{x^3}{6} + \frac{x^2.\frac{y^3}{6}.3}{6} - \frac{x^5}{120} \ldots = x + \frac{x^3}{6} + \frac{3x^5}{40} \ldots$

(iii) Assume a function is linear, as a first approximation.



(n) In solving $x^3 = 25 + x \ldots$ (1)

we note that $x^3 = 24 + x$ has solution $x = 3$

and so expect a solution of (1) close to 3.

We may write $f(x) \equiv x^3 - x - 25$, $f(3) = -1$, $f(4) = 35$

'Replacing the curve by a straight line' we have $x \approx 3 + \frac{1}{36} = 3.03$.

$f(3.03) = -0.21$.

Alternatively, write $x = 3 + h$ and "neglect h^2, etc."

$27 + 27h - 3 - h - 25 = 0$, $h = \frac{1}{26}$, $x = 3.04$, $f(3.04) = 0.05$.

In either case the process of approximation can be continued.

But note e.g.

that the solutions of $\frac{dy}{dx} = 1$ $y = 0$ for $x = 0$

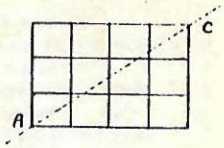
$\frac{dy}{dx} = 1 + 2y$ $y = 0$ for $x = 0$

$\frac{dy}{dx} = 1 + 2y + y^2$ $y = 0$ for $x = 0$

are different in form (after Polya). See Exercise 20.7, below.

Exercise 20

20.1 A rectangle 4 x 3 has one diagonal AC drawn.



This passes through 6 squares.

What is the general result for an m x n rectangle?

What is the analogous result for an m x n x p cuboid?

(A hint is given at the end of this Exercise).

20.2 To sum the series $1 + 2.\left(\frac{17}{20}\right) + 3.\left(\frac{17}{20}\right)^2 + \ldots$ write $\frac{17}{20} = x$ and consider the binominal expansion of $(1-x)^{-2}$ or the effect of differentiating $x + x^2 + x^3 + \ldots$

20.3 If $(n+1)$ positive integers are chosen from the set $\{1, 2, \ldots 2n\}$ prove that some pair of them has no factor in common, other than 1. (Walker (1977)).

20.4 A student writes :-

"The area of a Δ with sides a,b,c is either

$\frac{1}{2}\sqrt{s(s-a)(s-b)}$ or $\frac{1}{2}\sqrt{(s-a)(s-b)(s-c)}$ or $\frac{1}{2}\sqrt{s(s-a)(s-b)(s-c)}$

(where $s = \frac{a+b+c}{2}$) but I can't remember which, and I'm not sure whether the $\frac{1}{2}$ should be there or not." Can you help?

20.5 Find all the solutions in integers of (i) $x^2 + y^2 = 65$

(ii) $x^2 + y^2 = 4003$

(Hint. Think first!)

20.6 (Polya (1954) p.84) By multiplying $e^{x^2/2} = 1 + \frac{x^2}{2} + \frac{x^4}{2.4} + \frac{x^6}{2.3.8} \ldots$

and $\int_0^x e^{-t^2/2}\,dt = \frac{x}{1} - \frac{1}{2.3}x^3 + \frac{1}{2.4}\frac{x^5}{5} - \frac{1}{2.3.8}\cdot\frac{x^7}{7} \ldots\ldots$

find the first four terms of $y = e^{x^2/2}\int_0^x e^{-t^2/2}\,dt = x + \frac{x^3}{3} \ldots\ldots$

Guess the general term and use this information to find the series for y' and the differential equation satisfied by y. Then prove your guess.

20.7 Find the solutions of the three differential equations in (ii), p 105 above. Also give their series expansions.

20.8 (Putnam competition 1957)

Let a(n) be the number of representations of the positive integer n as sums of 1's and 2's taking order into account. (For example, since $4 = 1+1+2 = 1+2+1 = 2+1+1 = 2+2 = 1+1+1+1$, $a(4) = 5$).

Let b(n) be the number of representations of n as a sum of integers greater than 1, again taking order into account, and counting the summand n.

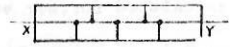
(e.g. $6 = 4+2 = 2+4 = 3+3 = 2+2+2$, $\quad b(6) = 5$)

Show that $a(n) = b(n+2)$ for each n.

Hint. Find a(n) in terms of a(n-1) and a(n-2), and find b(n) in terms of b(n-1), b(n-2), b(n-3) ..., b(2). Deduce that b(n) obeys the same recurrence relation as a(n).

Hint for problem 20.1. A useful analogous problem involves placing four rods each of length 3 units and three rods each of length 4 units side by side along the line XY.

Into how many segments is the line



XY divided by the junctions?

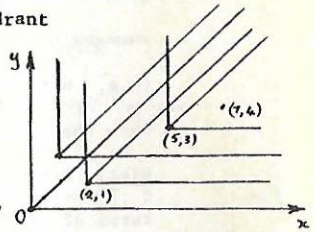
(See p. 99 above, 'transformation of a problem').

APPENDIX IV

A case history - how a proof was obtained

This is an outline account of how a student, S, solved the following problem. The solution was reached by stages, over a period of days and there were several false trails.(†)

The problem. We consider all points in the first quadrant with integer coordinates and delete those on the lines $x = 0$, $y = 0$ and $x = y$. The nearest points to (0,0) are now (2,1) and (1,2); we delete all points on the lines $x = 2$, $y = 1$, $x - y = 1$, $x = 1$, $y = 2$, $y - x = 1$, and find the pair of points nearest to (0,0) and so on. Considering only points for which $x > y$ we have (0,0), (2,1), (5,3), (7,4)..... Find the rule of the sequence.



S first calculated further values up to n = 6 (later 16) and observed $x_n - y_n = n$, on the line $x - y = n$ and $y_{n+1} \geq y_n + 1$ with equality only if $y_n + 1$ is not already an x..... (I)

$\Rightarrow x_{n+1} \geq x_n + 2$, 'in step' with y_n

Thus $y_{n+1} = y_n + 1$ or 2
$x_{n+1} = x_n + 2$ or 3 } in step

Because there are gaps in the x sequence, $y_{n+1} - y_n$ will never exceed 2 and will be 1 unless $y_n + 1$ is an x.

x_n	y_n	n
0	0	0
2	1	1
5	3	2
7	4	3
10	6	4
13	8	5
15	9	6
18	11	7
20	12	8
23	14	9
26	16	10
28	17	11
31	19	12
34	21	13
36	22	14
39	24	15
41	25	16

Some "Fibonacci sets" - e.g. 5,3,2, (13,8,5) were also noted by S - but this didn't produce any further insight

At this stage S remarked "This shows how to generate the sequence. I can't find an explicit formula for y_n and doubt if there is one."

(†) cf. Wheeler (1978) for an account of another problem solution.

S now decided to explore the asymptotic behaviour of x_n and y_n - i.e. by considering the 'average separation' of x's, to obtain an estimate of the magnitude of x_n :-

"Let average separation of x's be d, where $2 < d < 3$, $\Rightarrow$ that of y's is (d-1) (Note: The argument which follows led to a false conclusion, but nevertheless served a useful purpose):-

The expected value of $(y_{n+1} - y_n)$ is

2 × prob'. ($y_n + 1$ is an 'x') + 1 × prob'. ($y_n + 1$ is not an 'x').

$d - 1 = 2.\frac{1}{d} + 1.(1 - \frac{1}{d}) \Rightarrow d^2 - 2d - 1 = 0, d = 1 + \sqrt{2}$

This implies, for large n, $x_n \simeq dn = (1 + \sqrt{2})n$, and $y_n \simeq (\sqrt{2})n$

S now tried to get a recurrence relation for y_n.

From (I), $y_n = n + x^{-1}(y_n)$..... II where the second term means "number of (positive) x's less than y_n."

(for y_n would increase by 1 each time, as n does, were it not for the 'jumps' caused by presence of the x's.)

(S tried to use an 'x operator' on this, writing (wrongly) $x_{y_n} = x_n + y_n$ (abandoned) - this should have been $x_{(y_n - n)} < y_n$)

Then, by examining the table of results, he realised (II) could be also written as:-

$y_n = n +$ (no. of y's strictly between 0 and n) III

from which $y_{n+1} = y_n + 1 + \epsilon_n$ where $\epsilon_n = 1$ if n is a y, $= 0$ otherwise. } IV

(III) may be derived as follows:-

Let no. of x's strictly between 0 and y_n be N.

Then $N = y_n - n$ by (II).

Also x_N is just less than y_n i.e. $x_N < y_n < x_N + 1$

y_N is just less than $y_n - N = n$

So there are N values of y strictly between 0 and n.

S now returned to the asymptotic problem: If $y_n \doteq \lambda n$ for large n,

(III) gives :— $\lambda n = n + \frac{n}{\lambda} \Rightarrow \lambda^2 - \lambda - 1 = 0, \lambda = \frac{1+\sqrt{5}}{2} = 1.6180339$

So $y_{1000} \doteq 1618$

= 1000 + k where k is largest s.t. $y_k \leq 999$, k = 618 and so on,

"recursively".

Query: are 1618, 1000, 618 neighbouring Fibonacci nos?

(Conjecture: If n is a Fibonacci member, y_n is the next. e.g. $y_{13} = 21 = 13 + 8$

But $y_8 = 12 = 8 + 5-1$, so false).

Notes (i) This section contradicts earlier work suggesting $y_n = \sqrt{2}n$ (?)

(ii) S knew that large Fibonacci numbers could be found by

F_n = intof $(\frac{1}{\sqrt{5}}.\lambda^n)$ where λ has the above value.

(where intof(x) means "the largest integer $\leq$ x", sometimes written $[x]$).

This suggested the conjecture:-

y_n = intof (λn) .....(V)- or, perhaps, $\left\{\begin{array}{l}\text{intof } (\lambda n - 1) \\ \text{intof } (\lambda(n-1))\end{array}\right\}$?

(V) was verified for n = 1 - 8, 15, 16

S now explored (IV) using an electronic calculator and working backwards

from y_{1000} (for which (V) gives 1618).

$y_{1000} = 1000 + 618$; we need $y_{618} < 1000$ ((V) gives 999)

$y_{618} = 618 + 381$; we need $y_{381} < 618$ ((V) gives 616)

$y_{381} = 381 + 235$; we need $y_{235} < 381$ ((V) gives 380)

$y_{235} = 235 + 145$; we need $y_{145} < 235$ ((V) gives 234)

$y_{145} = 145 + 89$; we need $y_{89} < 145$ ((V) gives 144)

$y_{89} = 89 + 55$; we need $y_{55} < 89$ ((V) gives 88)

$y_{55} = 55 + 33$; we need $y_{33} < 55$ ((V) gives 53)

$y_{33} = 33 + 20$; we need $y_{20} < 33$ ((V) gives 32)

$y_{20} = 20 + 12$; we need $y_{12} < 20$ - but $y_{12} = 19$

Thus, from (III) the value of y_{1000} is derived, checking (V) for n = 1000, 618, . . etc.

S now wrote $v_n = \lambda n - y_n$ etc., without progress, and also tried to use mathematical induction. He was convinced the conjecture was true, but unable to prove it, at first, until this argument emerged:-

intof $(\lambda k) = n \Rightarrow n < \lambda k < n + 1$ i.e. $\frac{n}{\lambda} < k < \frac{n+1}{\lambda} = \frac{n}{\lambda} + \frac{1}{\lambda}$

Now ω_n = intof (λn) jumps by 2 when $n \to n + 1$ iff λn and $\lambda(n+1)$ enclose 2 integers.

i.e. iff $n + \frac{n}{\lambda}$ and $n + \frac{n}{\lambda} + 1 + \frac{1}{\lambda}$ enclose 2 integers (using $\lambda = 1 + \frac{1}{\lambda}$)

i.e. iff $\frac{n}{\lambda}$ and $\frac{n}{\lambda} + \frac{1}{\lambda}$ enclose one integer k

i.e. iff $\exists k$ s.t. $\omega_k = n$

Thus $\omega_{n+1} = \omega_n + 1 + \varepsilon'(n)$, where $\exists k, \omega_k = n \Leftrightarrow \varepsilon' = 1$, and $\varepsilon' = 0$ otherwise.

This is the same relation as that for y_n (i.e. IV)

and since $y_i = w_i$ for i = 1, 2, . . . 8 (checked). Hence $y_i \equiv w_i$ all i.

Notes

1. S's initial conclusion that "an explicit formula is improbable", was false.
2. He tried asymptotic behaviour as a 'second best' - but it led to a conjecture.
3. He tried several tricks of recurrence relations, with several false trails before achieving "partial success" - as he regarded it - with (IV).
4. Reconsideration of asymptotic behaviour gave a conflicting result $y_n \doteq \lambda n$. (Later examination of table as far as $y_{16} = 25$ gives 9 gaps of 2, 7 gaps of 1, estimating (d-1) as

   $2.\frac{9}{16} + 1.\frac{7}{16} = 1\frac{9}{16} = 1.5625$ (cf 1.62 and 1.41)).
5. The proof of conjecture (V) was conclusive, though S was now unhappy about the unlocated error in the argument leading to $y_n \doteq \sqrt{2}.n$. He suspected this was due to unrecognised assumptions in the conditional probability argument, and tried to revise this as below.

6. The 'Fibonacci' conjectures were incorrect, despite the appearance of $\lambda = \frac{1+\sqrt{5}}{2}$, yet the ideas associated with Fibonacci sequences - and experience with calculations involving 'intof' - were helpful.

S's Re-examination of the conflicting results ($y_n \doteq \lambda n$, (from III), $y_n \doteq \sqrt{2n}$, (from probability, $E(y_{n+1} - y_n)$). (Later version).

(i) The actual separation between ω_n and ω_{n+1} is not λ but is

intof$(\lambda(n+1))$ - intof (λn)

= 1 + number of integers in $\left[\frac{n}{\lambda}, \frac{n}{\lambda} + \frac{1}{\lambda}\right]$

So $E(\omega_{n+1} - \omega_n) = 1 + E(\exists\ k \text{ with } n < \lambda k < n+1) = 1 + \frac{1}{\lambda} = \lambda$, which is consistent.

(ii) Let probability (randomly chosen no. is a "y") be $\frac{1}{c}$, and . . . is an "x" be $\frac{1}{c+1}$

i.e. Average spacing of "y"s is $c = E(y_{n+1} - y_n)$.

Then $\frac{1}{c} + \frac{1}{c+1} = 1 \Rightarrow c^2 - c - 1 = 0$, $c = \lambda = \frac{1+\sqrt{5}}{2}$

S also noted, from the numerical values, 2 conjectures:-

(i) $\delta y = y_{n+1} - y_n = 1 \Rightarrow y_{n+2} - y_{n+1} \neq 1$.

(ii) $y_{n+1} - y_n = 2 \Rightarrow y_{n+2} - y_{n+1} = 1$ or 2. (But there are not 3 jumps of 2 in succession).

These were proved as follows:-

(i) $\delta y = 1 \Rightarrow \exists$ one integer between $n\lambda$ and $(n+1)\lambda$.

But $\exists$ 3 integers between $n\lambda$ and $(n+2)\lambda$, since $2\lambda = 3.236\ldots$

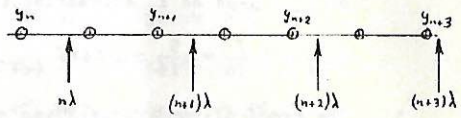
(ii) $\delta^2 y = 2 \Rightarrow \exists$ 2 integers $k, k+1$ between $n\lambda$ and $(n+1)\lambda$.

3 successive gaps of 2

$\Rightarrow 2\lambda > 3$ (true)

and $3\lambda > 5$ (false)

since $\lambda < 5/3 = 1.6667$



A Formal proof

The sequences x_n, y_n are defined by

$x_1 = 2$, $y_1 = 1$

$y_{n+1} = y_n + 1$, except that if $y_n + 1 = x_k$ for $k < n$, then $y_{n+1} = y_n + 2$

$x_n = y_n + n$ } (1)

Find expressions for x_n, y_n.

Clearly it is sufficient to consider y_n. We prove $y_n = \text{intof}(\lambda n)$ where λ is the positive root of $t^2 - t - 1 = 0$.

From (1), $y_n = n + k$ (2) where k is the number of values of $x_i \leq y_{n-1} + 1$

i.e. the largest i for which $x_i < y_n$.

But since $x_k = y_k + k$, k is also the largest i for which $y_i < n$. (3)

Thus $y_{n+1} = y_n + 1 + \varepsilon_n$ (4) where $\begin{cases} \varepsilon_n = 1 \text{ if } n = y_s \text{ for some } s. \\ = 0 \text{ otherwise} \end{cases}$

Now consider $\omega_n = \text{intof}(\lambda n)$ where $\lambda^2 - \lambda - 1 = 0$, $= \frac{1+\sqrt{5}}{2} = 1.618\ldots$

$\omega_{n+1} - \omega_n$ = no. of integers in $(\lambda n, \lambda n + \lambda)$ i.e. in

$(n + \frac{n}{\lambda}, n+1 + \frac{n}{\lambda} + \frac{1}{\lambda})$, using $\lambda = 1 + \frac{1}{\lambda}$

= 1 + no. of integers in $(\frac{n}{\lambda}, \frac{n}{\lambda} + \frac{1}{\lambda})$

Now $\text{intof}(\lambda k) = n \Rightarrow n < \lambda k < n+1 \Rightarrow \frac{n}{\lambda} < k < \frac{n}{\lambda} + \frac{1}{\lambda}$

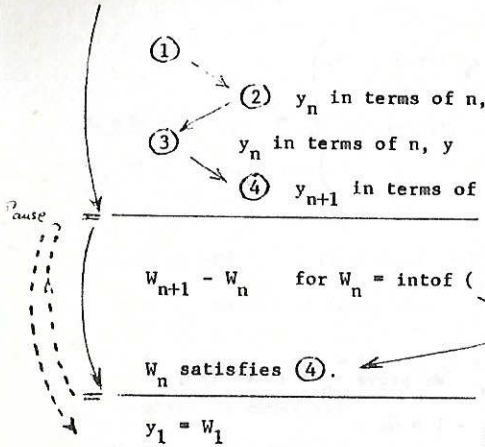
Thus $\omega_{n+1} - \omega_n = 1 + \varepsilon'_n$ where $\begin{cases} \varepsilon'_n = 1 \text{ if } \exists k \text{ s.t. } \omega_k = n \\ = 0 \text{ otherwise.} \end{cases}$

This is the same relation as (4), and since $y_1 = 1 = \omega_1 = \text{intof}(1.618)$, $y_n = \omega_n$ for all n.

Hence $y_n = \text{intof}(\lambda n)$ where λ is the positive root of $t^2 - t - 1 = 0$.

Structure of the proof

(State ultimate goal: definition of y_n



Note "Where does the conjecture W_n = intof (λn) come from ?" - there is no hint in the formal proof of why this is relevant.

Hints and Solutions

Ex.1.1 (p.3) Square specified by size, and position of top L.H. corner

4 x 4 = 16 positions for a 2 x 2 square on a 5 x 5 board.

1.2 Even - see Ex 2.1, p.5. Prime. see p.5 Example (ii) and p.6 Example 2.2

1.3 (p.4) "Traditional" proof uses congruent Δ's. Two line segments are shown collinear so theorems on "area of Δ's between parallels" may be used.

Similar Δ proofs use the right-angle explicitly.

Ex.2.1 (p.5) $2n + 2$, the $(n+1)^{th}$ even no. 2.2 $f(c) = a_n (b + kf(b))^n + \ldots$

$= a_n b^n + a_{n-1} b + \ldots + a_0 +$ terms involving f(b)

= multiple of f(b).

2.3 $R_5 = 16$, $R_6 = 31$ ($R_7 = 57$, $R_8 = 99$).
[See Ex 17.9, p 84.]

2.4 $R_5 = 16$, $R_6 = 22$, $R_n = \frac{n(n+1)}{2} + 1$.

Ex.3 (p.7) See 1.1 above. $\exists$ $(n + 1 - a)(n + 1 - a)$ positions for an a x a square on n x n board.

Since a runs from 1 to n, total is $n^2 + (n-1)^2 + (n-2)^2 + \ldots + 2^2 + 1^2 = \frac{1}{6} n (n+1)(2n+1)$.

Ex.4.1 (p.11) All T ; converse of (c) and (e) T; (a) $\{2, 4\}$, (b) [illegible] (d) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$

4.2 (a) Assuming an equivalent result. (Unless $\sin^2\theta + \cos^2\theta = 1$ is proved by similar Δ's, which is equivalent to Pythagoras). c.f. Prove 1 = 4 by assuming 1 = 2 and squaring.

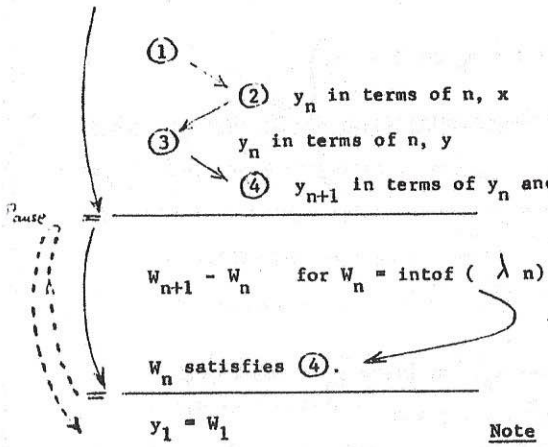
(b) Failure to deduce contradiction is not a proof.

(c) Consideration of special cases only. (c.f. "I don't like Canadians; I met one once.).

(d) Overdependence on pictures - see also p.13.

Structure of the proof

(State ultimate goal: definition of y_n



Note "Where does the conjecture W_n = intof (λn) come from ?" - there is no hint in the formal proof of why this is relevant.

Hints and Solutions

Ex.1.1 (p.3) Square specified by size, and position of top L.H. corner

4 x 4 = 16 positions for a 2 x 2 square on a 5 x 5 board.

1.2 Even - see Ex 2.1, p.5. Prime. see p.5 Example (ii) and p.6 Example 2.2

1.3 (p.4) "Traditional" proof uses congruent Δ's. Two line segments are shown collinear so theorems on "area of Δ's between parallels" may be used.

Similar Δ proofs use the right-angle explicitly.

Ex.2.1 (p.5) $2n + 2$, the $(n+1)^{th}$ even no. 2.2 $f(c) = a_n (b + kf(b))^n + \ldots$

$= a_n b^n + a_{n-1} b + \ldots + a_0 +$ terms involving f(b)

= multiple of f(b).

2.3 $R_5 = 16$, $R_6 = 31$ ($R_7 = 57$, $R_8 = 99$).
[See Ex 17.9, p 84.]

2.4 $R_5 = 16$, $R_6 = 22$, $R_n = \frac{n(n+1)}{2} + 1$.

Ex.3 (p.7) See 1.1 above. $\exists$ $(n + 1 - a)(n + 1 - a)$ positions for an a x a square on n x n board.

Since a runs from 1 to n, total is $n^2 + (n-1)^2 + (n-2)^2 + \ldots + 2^2 + 1^2 = \frac{1}{6} n (n+1)(2n+1)$.

Ex.4.1 (p.11) All T ; converse of (c) and (e) T; (a) $\{2, 4\}$, (b) ~~T~~ (d) $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}$

4.2 (a) Assuming an equivalent result. (Unless $\sin^2\theta + \cos^2\theta = 1$ is proved by similar Δ's, which is equivalent to Pythagoras). c.f. Prove 1 = 4 by assuming 1 = 2 and squaring.

(b) Failure to deduce contradiction is not a proof.

(c) Consideration of special cases only. (c.f. "I don't like Canadians; I met one once.).

(d) Overdependence on pictures - see also p.13.

(c) Proving the converse. (In fact, the theorem is false. p 96.)

(f) Theorem states, "L.H.S. cgt. and sum is -1". Proof assumes convergence.

4.3 (p.12) (b) shows only possible solution is (2, 1) - but does not check it satisfies both equations. (c.f. "Solve $\frac{1}{x-3} = \frac{1}{x^2-5x+6}$ ").

(c) shows (2, 1) is a solution, but not that there are no others.

(c.f. "Solve $x^2 + y^2 = 1$, $y = x-1$ ").

(d) Sometimes criticised "because inaccurate" - but c.f. solving $x^3 - 5x = 1$ by graph or iteratively with a calculator - as accurately as we please.

Provided we accept that linear equations are represented by st.lines,

(a) is the only acceptable proof (though (b) could easily be amended).

4.4 (a) α in complex, β in real, γ in positive reals.

(b) $x = 6$. Irreversible steps give $x = -2$ which does not satisfy the equation.

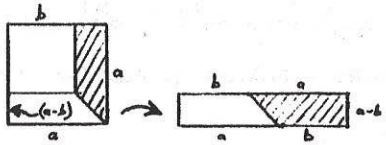
(c) Confusion of theorem and converse (write $p = q\theta$, $s = r\theta$ etc.).

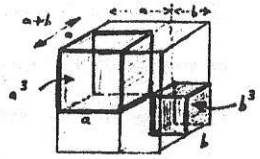
Ex.5.1 (p.14) (a) Axis of symmetry PR $\Rightarrow$ sides equal. DP, SB inclined at $\tan^{-1}2$, $\tan^{-1}\frac{1}{2}$ to DC $\Rightarrow$ angles 143.14°, 126.86°.

(b) Gradient SR = $^3/_8$, of QR = $^2/_5$. PQRS is parallelogram, unit area.

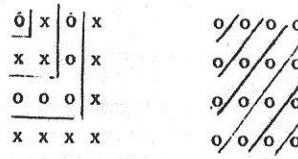
5.2 (a) True - proof by areas: (b) False - see Ex. 10.6 p.40.

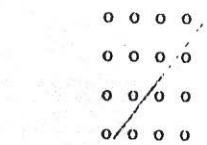
Ex.6.1 (p.15)
$$(a+b)^3 = a^3 + b^3 + 3a^2b + 3ab^2$$
$$a^3 + b^3 = (a+b)(a^2 - ab + b^2) = (a+b)a^2 + (a+b)b^2 - a(ab) - b(ab)$$





6.2





$1 + 3 + 5 + 7 = 4^2$. $1 + 2 + 3 + 4 + 3 + 2 + 1 = 4^2$ $T_4 + T_3 = 4^2$.

Ex.7.1 (p.17) Using (j2), $xy = f^2 \Rightarrow x + y \geq 2f > 2d = x + y$, (contrad^n.) (of $x + y$)

7.2 Similarly if $xy = d^2$ and suppose min. value is $2f$, $f < d$, when $x \neq y$.

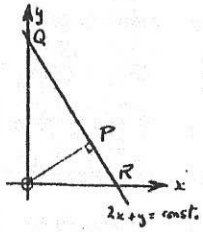
By (j 3) $x + y = 2f \Rightarrow xy \leq f^2 < d^2 = xy$, (contrad^n).

7.3 $2(x^2 + y^2) = (x+y)^2 + (x-y)^2 \geq (x+y)^2$ with equality $x = y$ (i.e. j1)

$(x + y)^2 = 4xy + (x - y)^2 \geq 4xy$ with equality $x = y$ (i.e. j2 & j3 similarly).

7.4 Let $x + y + z = c$. For fixed z, $x + y = c - z = \text{const.}$ and xy will be greatest when $x = y$. Thus if $x \neq y$ we can increase xyz by leaving z unaltered and equalising x and y.

7.5



OP perp. QR $\Rightarrow$ OP is $y = \frac{1}{2}x$
If $2x + y = c$,
then $(x^2 + y^2)_{min} = 4c^2 + c^2 = 5c^2$.

Alternatively,
Consider five numbers $\frac{x}{2}, \frac{x}{2}, \frac{x}{2}, \frac{x}{2}, y$ whose sum is fixed.
By analogy with (j1) and 7.4 Σ squares least when all are equal.

Ex. 8.1 (p.30) 3, 4, 5, 7. (1, 2, 6 are $\mathcal{B} \Rightarrow$ S).

8.2 $f = A(x + \frac{B}{2A})^2 + \frac{4AC - B^2}{4A} > 0$ all $x \Leftrightarrow A > 0$ and $B^2 < 4AC$. N and S.

8.3 N, N and S, S, N and S, neither N nor S (rectangle, rhombus), N, N.

Ex.9 (p.38) (Partial answers)

9.1 y has no brothers, y has a sister z.

9.3 (a) Every perfect square is the difference of two squares. T.
Odd square $= 2n + 1 = (n+1)^2 - n^2$
Even square $= 4^k(2n+1) = [2^k(n+1)]^2 - [2^k(n)]^2$

(b) False. For suff. large x, $x^2 < x^2 + y^2 < (x+1)^2$.

9.8 T, F, T, F (e.g. $q = 1$.).

9.9 (a) $\forall p, \forall q$, $q \neq p + 2$ (b) $\forall q\ \exists p$ $q \neq p + 2$

Ex.10.1 (p.40) True N = 1 - 5, F (6) = 7.

10.2 (α) is true for n prime (but ${}_4C_2$ is not mult. of 4).

$pC_k = \frac{p(p-1)\ldots(p+1-k)}{k!}$ and $p \nmid k!$

(β) is false e.g. $9^C5 = 126 \neq M(5)$ - or use n = 3.

10.3 $(a_o\, b)_o\, c = c$, $a_o\, (b_o\, c) = a$.

10.4 (α) $2^4 - 2 = 14 \neq M(4)$ (β) $2^9 - 2 = 510 \neq M(9)$. In fact $n^k - n = M(k)$ if k prime (Fermat); see Stewart (1975) p. 39.

10.5 $7 = 2^2 + 1^2 + 1^2 + 1^2$ by exhaustion.

10.6

If I is in-centre of ΔABC

$\frac{IX}{XB'} = \frac{1}{\sqrt{2}}$, $\frac{IY}{YB'} = 1$ etc.

Ex.11.1 (p.41) Let m = ef, e even, f odd, f > 1.

$N = 2^m + 1 = (2^e)^f + 1 = x^f + 1 = (x+1)(x^{f-1} - x^{f-2} + \ldots\ldots + 1)$, which has factor (x + 1)

11.2 Neither of x, y is 3k. If both of form 3k+1, xy of same form.

If both of form 3k + 2, $xy = (3k_1 + 2)(3k_2 + 2) = 3k_3 + 1$.

11.3 $\Rightarrow$). Suppose f not 1-1, $f(\underline{x}) = f(\underline{y})$, $\underline{x} \neq \underline{y}$, $f(\underline{x} - \underline{y}) = \underline{0}$ and $(\underline{x} - \underline{y}) \in \ker f$.

$\Leftarrow$). Suppose $\underline{a} \in \ker f$, $\underline{a} \neq \underline{0}$, $\Rightarrow f(\underline{x} + \underline{a}) = f(\underline{x}) + f(\underline{a}) = f(\underline{x}) + \underline{0} = f(\underline{x})$, $\Rightarrow$ f not 1-1.

Ex. 12.1 (p61). $t^2 = t + 1$. $u_n = A\alpha^n + B\beta^n$ is a solution

$\left.\begin{array}{l} n = 1.\ 1 = A\alpha + B\beta \\ n = 2.\ 1 = A\alpha^2 + B\beta^2 \end{array}\right\} \Rightarrow A = -B = \frac{1}{\sqrt{5}}$

u_n uniquely determined by u_1, u_2 $\Rightarrow$ this is only solution.

12.2 (α) $\theta_1 - \theta_2$ (light ray), (β) strings at 120° at equilibrium $\Rightarrow$ min. energy.

(γ) ΔAPP_1 equilateral. Min. when B_1, P_1, P_2, C collinear $\Rightarrow \widehat{APC} = 120°$.

(δ) If $\perp^r$ from Y to VW is YA', etc., YA + YB + YC > YA' + YB' + YC' = XA+XB+XC (P.47 Ch.7)

Appendix

Ex.14.1 (p.66) Induction on x. x = 1 ✓. Assume $yx + zx = (y + z)x$.

Then $y.S(x) + z.S(x) = (yx + y) + (zx + z) = yx + zx + y + z$ (proved)

$= (y + z).x + (y + z)$ (inclination hypothesis)

$= (y + z).S(x)$. Hence by M.1.

For xy = yx prove x.1 = 1.x by induction on x, then use induction on y.

14.2 p = (x,y) q = (s,t). Equality iff xt = ys. p + q = (xt + ys, yt), pq = (xs, yt)

O = (0,y), 1 = (y,y), -p = (-x,y), $p^{-1} = (y,x)$ $[x \neq 0]$.

14.3 Similarly z = (x,y) w = (s.t). Equality iff x = s and y = t, z + w = (x + s, y + t)

z.w = (xs - yt, xt + ys). Proofs are verification. $\underline{1} \equiv (1,0)$,

$z^{-1} \equiv \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right)$

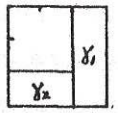
Ex.15.1 (p.78) $\Sigma\alpha + 2\beta = 1$, $\Sigma\alpha = \frac{1}{5}$ $\frac{1}{3} + (\frac{1}{3})^2 + \ldots = \frac{1}{2}$

15.2 $\Sigma\alpha = 1 = \frac{1}{5}(1 + \frac{4}{5} + (\frac{4}{5})^2 + \ldots.)$

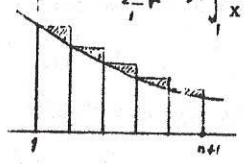
So $\frac{4}{5} + (\frac{4}{5})^2 + \ldots. = 5 - 1 = 4$.

$\Sigma\gamma = 1 = \frac{1}{3}(1 + \frac{2}{3} + (\frac{2}{3})^2$

$\Rightarrow \frac{2}{3} + (\frac{2}{3})^2 + \ldots = 2$.



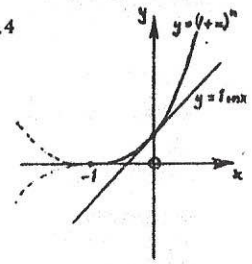
15.3 $\sum_1^n \frac{1}{r} > \int_1^{n+1} \frac{1}{x}dx = \log_e(n+1)$; difference = shaded area, which ↑ with n, < 1 (would all fit into the sq. on [1,2]) and is > ½, (each area is larger than a Δ).



$\gamma \simeq \frac{1}{2}$. Calculating the first, second, third "triangles" accurately gives $\gamma > 0.557, 0.568, 0.572$.

($\gamma = 0.577215..$).

15.4



$\frac{dy}{dx} = n(1+x)^{n-1} = n$ when x = 0

$\frac{d^2y}{dx^2} = n(n-1)(1+x)^{n-2} > 0$, n > 1, so curve lies above tgt. [Also easily proved by M.I, p.35.]

Ex.16 (p.79).

16.3 P_4 is $2^4 \geqslant 4^2$ (true). $P_k \Rightarrow P_{k+1}$ for $k \geqslant 3$, but since P_3 is false we must start off the induction with P_4.

16.5 Let P'_k be $(1+x)^k > 1+kx$. P'_2 is true, $x \neq 0$,

$P'_k \Rightarrow P'_{k+1}$ Hence P'_k, which $\Rightarrow (1+x)^k > kx$.

16.6 $\frac{n+1}{2n}$

16.8 $f(k+1) = 9.f(k) + 8$ etc. Note also two direct proofs:-

(i) $3^{2n} - 1 = (3^n + 1)(3^n - 1)$, two consecutive even integers, one being $M(4)$.

(ii) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}\,b + \ldots + b^n)$ with $a = 9$, $b = 1$.

16.9 Two cases. $2^{2m+1} + 1$ is multiple of 3, $2^{2m} - 1$ is multiple of 3.

16.10 Verify P_1, P_2. Write $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$ and note that α, β satisfy $t^2 - t - 1 = 0$, ie. $t^2 = t + 1$. Use P_k and P_{k-1} to prove P_{k+1}.

16.11 - 14 See standard texts, which often give alternative direct proofs.

16.15 Integration by parts gives $I_n = \left[-e^{-x}.x^n\right]_0^\infty - \int_0^\infty (-e^{-x})\, nx^{n-1} dx = n\, I_{n-1}$.

16.16 Alternatively write $r(r+1)(r+2) = \frac{r(r+1)(r+2)(r+3)}{4} - \frac{(r-1)r(r+1)(r+2)}{4}$ and sum from 1 to n. This is a useful method and a useful result.

(See. Ex 17.6, 17.9 pp 83, 84, and (4), p100).

16.18 When a new line is added, retain the colouring on one side of it and reverse the colouring on the other. Hence $P_k \Rightarrow P_{k+1}$

Ex.17.1 (p83). $u_{n+1} - u_n = V_{n+1} - V_n$. Thus $u_n = V_n \Rightarrow u_{n+1} = V_{n+1}$. $u_1 = V_1$.

17.2 $a = \sqrt{3} + 1$, $b = \sqrt{3} - 1$, $n = 2k + 1$.
$f(k+1) = 6(a^{2k} + b^{2k}) + 2\, f(k)$, and $a^{2k} + 2^{2k}$ is mult. of 2^k, since only even powers of $\sqrt{3}$ occur.

17.4. P_1 (def^n). P_k $u_{n+k} = u_{n-1}u_k + u_n u_{k+1}$; P_{k-1} $u_{n+k-1} = u_{n-1}u_{k-1} + u_n u_k$ } adding gives P_{k+1}.

(From this we have u_{ns} divisible by u_n, and so u_n prime $\Rightarrow$ n prime)

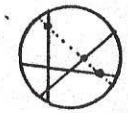
17.5 (p83) Suppose $(n-1)a^n + b^n > n a^{n-1} b$. P_n

Then $na^{n+1} + b^{n+1} = b^{n+1} + a^{n+1} + (n-1)a^{n+1} > b^{n+1} + a^{n+1} + a(n-1)a^n + b^n) - ab^n$
$> na^n b + b^{n+1} + a^{n+1} - ab^n + a^n b - a^n b = (n+1)a^n b + (a-b)(a^n - b^n)$
$> (n+1)a^n b$ ie P_{n+1}

Now $(a_1 + a_2 + \ldots + a_{n-1}) + a_n > n\left(\frac{a_1 + \ldots + a_{n-1}}{n-1}\right)^{\frac{n-1}{n}} \cdot (a_n)^{\frac{1}{n}}$

i.e. $\left(\frac{a_1 + \ldots + a_n}{n}\right)^n > a_n \left(\frac{a_1 + \ldots + a_{n-1}}{n-1}\right)^{n-1}$, which, by M.I on n, $> a_n a_{n-1} \ldots a_1$.

17.6



Let $R_k = \frac{1}{2}(k^2 + k) + 1$. Consider a plane cross section as shown. The addition of an extra plane implies the addition of an extra line (shown dotted) which meets each of the other k lines and so is divided into (k+1) segments, each of which cuts through an existing region:

Thus $R_{k+1} = k + 1 + R_k = \frac{1}{2}(k+1)(k+2) + 1$, as required. Similarly each of these regions of a plane cross section produces one extra volume (piece) when the corresponding plane cut is made.

i.e. $V_{k+1} = V_k + R_k$

Thus $V_{k+1} = \frac{1}{6}\left((k+1)^3 + 5(k+1) + 6\right)$ as required.

17.7 (c) $(n+1)^7 - (n+1) - (n^7 - n) = (n+1)^7 - n^7 - 1 = n^7 + 7n^6 + \ldots + 1 - n^7 - 1$

= Multiple of 7, since every binomial coeff. ${}_7C_i$, for $6 \geqslant i \geqslant 2$, is $\equiv 0 (7)$.

Thus $P_n \Rightarrow P_{n+7}$. P_1 is evident.

Note This result may also be proved by exhaustion, or using Fermat's theorem. (See p.32 and Stewart (1975) p.39)

17.8 $D^{n+1}(e^{x^2/2}) - D(u_n(x).e^{x^2/2}) = u_n'(x).e^{x^2/2} + u_n(x).x.e^{x^2/2}$ i.e. $u_{n+1} = u_n' + x u_n$ ①

$D^n(x e^{x^2/2}) = u_{n+1}(x).e^{x^2/2} = x u_n(x).e^{x^2/2} + u_{n-1}(x)e^{x^2/2}.n$, by Leibnitz' theorem. (Ex.16.14, p.80)

i.e. $u_{n+1} = x u_n + n u_{n-1}$ ② Hence $u_n' = n u_{n-1}$ ③

$\therefore u_{n+1} = (n+1)u_n$ (③) $= u_n'' + x u_n' + 1.u_n$ using ①. i.e. $u_n'' + x u_n' - n u_n = 0$,

$D^2 y + x.Dy - ny = 0$ ④. From ①, if u_n is polynomial, $\partial^o n$, 1st two coeffs 1 and 0, so is u_{n+1}. But $u_1 = x$. ✓

Put $u_n \equiv y = x^n + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} + \ldots$

From ③ $(r+2)(r+1)a_{r+2} + r a_r - n a_r = 0$ (coeff x^r).

Hence $n(n-1)a_n = 2a_{n-2}$. $a_{n-2} = \frac{n(n-1)}{2}$
$(n-2)(n-3)a_{n-2} = 4.a_{n-4}$ $a_{n-4} = \frac{n(n-1)(n-2)(n-3)}{2.4}$ } and other (odd) coeffs. zero

..... etc.

17.9 (a) Join $(n-r)$ points on one side of $P_{n+1}P_r$ to $(r-1)$ on the other.

(b) No. of regions = $n\sum_1^n(r-1) - \sum_1^n r(r-1) + \sum_1^n 1 = \frac{n^2(n-1)}{2} - \frac{n(n-1)(2n+1)}{3} + n = n + \frac{n(n-1)(n-2)}{6}$

(c) Since $R_1 = 1$, we have $R_n = 1 + \sum_1^{n-1} \frac{r(r-1)(r-2)}{6} + \sum_1^{n-1} r = 1 + \frac{(n-3)(n-2)(n-1)n}{24} + \frac{(n-1)n}{2}$

$= {}_nC_4 + {}_nC_2 + 1.$

(Part (c) could also be proved by M.I.)
The form of this result suggests an alternative proof:-

There is initially one region inside the circle.

As each chord is added it produces additional regions, one more than the number of existing chords it meets. When all chords drawn, $N_1 + N_2$ regions have been added, where $N_1 = {}_nC_2$ = number of chords and $N_2 = {}_nC_4$ = no. of interior points of intersection (meets of diagonals of the ${}_nC_4$ quadrilaterals). i.e. total $= 1 + {}_nC_2 + {}_nC_4$.

17.10 Induction on n. P_1, P_2 true, since $0 \le 0$ and $2a - a^2 \le 1$ by $(a-1)^2 \ge 0$.

Let $ak - a^k \le k-1$. (P_k) Then $a(k+1) - a^{k+1} \le \ldots\ldots k(2a-a^2) \le k$. (by P_2).

Alternatively.

(a) To prove $n(a-1) \le a^n - 1 \equiv (a-1)(a^{n-1} + a^{n-2} + \ldots + 1)$

For $a \gtrless 1$, req. to prove $n \lesseqgtr a^{n-1} + a^{n-2} + \ldots + 1$.

(b) $f(a) = ak - a^k$. $f'(a) \lesseqgtr 0, a \gtrless 1$, so max. value $= f(1) = k-1$.

(c) Put $a = 1 + x$ and use (k), p 37.

Ex 18.1 (p 84) $2u_{n+1}u_n - u_n^2 = A^2 \Rightarrow 2(u_{n+1} - A)u_n = (A - u_n)^2 \ge 0$ (†)

so that $u_{n+1} \ge A$ (whether or not $u_n > A$).

Also $2(u_{n+1} - u_n)u_n = A^2 - u_n^2 \le 0, \Rightarrow u_{n+1} \le u_n$.

$u_n \downarrow$, bdd. below, and so $\longrightarrow$ limit ℓ, where $2\ell^2 - \ell^2 = A^2$, $\ell = A$.

Last part from (†).

18.2 $\frac{(m.\frac{x}{m} + n.\frac{y}{n})}{m+n} \ge \left(\frac{x^m}{m^m} \cdot \frac{y^n}{n^n}\right)^{\frac{1}{m+n}}$ etc

18.3 e.g. $28!$ contains the factor 3, $9 + 3 + 1 = 13$ times.

If $\left[x + \frac{1}{p}\right] = \lambda + 1$ then $\epsilon > \frac{p-1}{p} \ge \frac{1}{2}$ and so $[2\lambda + 2\epsilon] = 2\lambda + 1$.

Any factor p of denominator occurs with equal or greater multiplicity in the numerator.

Ex. 19.1 (p. 93) $(F_i - 1) = (F_j - 1)^{2^{i-j}} = M_{\text{ult.}}(F_j) + 1$. Thus any common factor of F_i, F_j is a factor of 2.

Suppose $\exists$ only k primes. Then at least 2 of $F_1, F_2, F_3, \ldots F_{k+1}$ would have a prime factor in common.

19.2 $(4a+1)(4b+1)$ of form $4k+1$. So $4n + 3$ must contain at least one factor $4k + 3$ ($k \neq 0$) (unless it is prime). Rest of argument like Euclids' proof.

19.3 Let $N = 2.3.5.7.\ldots 97.101$, i.e. product of all primes ≤ 101

Then $N+2, N+3, N+4, \ldots N+101$ are all composite. (It is simpler to use $N = 101!$)

Ex. 20.1 (p 106) Count one square for each horiz. and each vert. line met after leaving A, (except at C). This gives $m + n - 1$ squares, unless m, n have common factor h, when result is $m + n - h$. In 3-D case, no. $= m + n + p - (m,n) - (n, p) - (p, m) + (m, n, p)$, where $(m, n) =$ hcf. (m, n) etc.

20.2 $D\left(\frac{1}{1-x}\right) = (1-x)^{-2}$. (We assume term by term differentiation is permissible - or we may work with $D\left(\frac{1-x^n}{1-x}\right)$).

20.3 Into n boxes place 1, 2; 3, 4; etc.

Now remove $(n + 1)$ numbers. At least one box must be empty - the numbers k, k+1 are coprime. See Walker (1977)

20.4 1st not symmetric a, b, c; 1st, 2nd wrong dimensions; $a = b = c \Rightarrow \Delta = \frac{a^2\sqrt{3}}{4}$

i.e. "$\frac{1}{2}$" should be omitted in 3rd.

20.5 (8, 1), (1, 8), (7, 4), (4, 7) by exhaustion. No solutions $4n + 3$ (p. 41).

20.6 $y = x + \frac{x^3}{3} + \frac{x^5}{15} + \frac{x^7}{3.5.7}$, $y' = 1 + xy$. Verify product satisfies D.E.

Both product and series are zero, $x = 0$.

20.7 $y = x$, $\log(1+2y) = x + C \Rightarrow y = \frac{1}{2}\left(x + \frac{x^2}{2} + \frac{x^3}{6} \ldots\right)$

$1 + y = z$, $\frac{dz}{dx} = z^2$, $z = \frac{1}{1-x}$, $y = x + x^2 + x^3 + \ldots$

20.8 (p.107) $3 = 1+2 = 2+1 = 1+1+1$ $\left(a(3) = 3\right)$

$2 = 1+1$ $\left(a(2) = 2\right)$

In writing 4 as sum of 1's and 2's we either begin $4 = 2+\ldots$, a(2) ways

or $4 = 1+\ldots$, a(3) ways

Thus $a(4) = a(2) + a(3)$ and similarly $a(n) = a(n-1) + a(n-2)$.

Likewise in writing 7 as sum of integers > 1, we begin

$7 = 2 + \ldots$, b (5) ways

$= 3 + \ldots$, b (4) ways

$= 4 + \ldots$, b (3) ways

$= 5 + \ldots$, b (2) ways

i.e. $b(7) = b(5) + b(4) + b(3) + b(2) + 1$, and similarly for $b(n)$

Thus $b(n) - b(n-1) = b(n-2)$. But $b(3) = a(1)$, $b(4) = a(2)$, Hence...

REFERENCES

APPEL, K. and HAKEN, W. "The Solution of the four colour map problem." Scientific American, October 1977, pp. 108-121.

AVITAL, S. and HANSEN, R.T. "So simple and so rich: the mailbox principle", Mathematics Teaching, No. 76, September 1976 .

BELL, E.T. Mathematics - Queen and Servant of Science. Bell, 1952.

BLUMENTHAL, L.M. A modern view of geometry. Freeman, 1961.

BOLTYANSKI, V.G. Equivalent and Equidecomposable figures. D.C. Heath, 1963.

COURANT, R. and ROBBINS, H. What is Mathematics? Oxford U.P., N. York 1941.

ESTERMANN, T. "A proof of the irrationality of $\sqrt{2}$." Math. Gaz. 408, June 1975. p. 110.

EVES, H. and NEWSOME, C. Introduction to the foundations and fundamental concepts of mathematics. Holt Rinehart, 1964 .

FETISOV, A.I. Proof in geometry. D.C. Heath, 1963.

FLETCHER, T.J. "Doing without calculus." Math. Gaz. 391. February 1971, pp. 4-17.

FLETCHER, T.J. Linear algebra through its applications. Van Nostrand, 1972 .

GALILEO, G. Dialogue concerning Two New Sciences. Dover, 1954..

HARDY, G.H., LITTLEWOOD, J.E. and POLYA, G. Inequalities. C.U.P., 1934..

HEATH, Sir T.L. The Thirteen Books of Euclid's Elements. Vol. I. Dover, 1926.

HIRST, K.E. and RHODES, F. Conceptual models in mathematics. Allen and Unwin, 1971.

KAC, M. and ULAM, S. Mathematics and Logic. Penguin Books, 1971 .

KLEIN, F. Elementary mathematics from the advanced standpoint. Vols. I and II. Dover, 1939.

LAKATOS, I. Proofs and refutations: the logic of mathematical discovery. C.U.P., 1976.

McCANN, G. "Pythagoras without squares". Mathematics Teaching No. 75. June 1976 .

MAXWELL, E.A. Fallacies in mathematics. C.U.P., 1959 .

MOSES, S. The art of problem solving. Transworld, 1974.

NAGEL, E. and NEWMAN, J.R. Gödel's proof. R.K.P., 1971 .

20.8 (p.107) $3 = 1+2 = 2+1 = 1+1+1 \quad (a(3) = 3)$

$2 = 1+1 \quad (a(2) = 2)$

In writing 4 as sum of 1's and 2's we either begin $4 = 2+\ldots$, a(2) ways

or $4 = 1+\ldots$, a(3) ways

Thus $a(4) = a(2) + a(3)$ and similarly $a(n) = a(n-1) + a(n-2)$.

Likewise in writing 7 as sum of integers > 1, we begin

$7 = 2 + \ldots$, b (5) ways

$= 3 + \ldots$, b (4) ways

$= 4 + \ldots$, b (3) ways

$= 5 + \ldots$, b (2) ways

i.e. $b(7) = b(5) + b(4) + b(3) + b(2) + 1$, and similarly for $b(n)$

Thus $b(n) - b(n-1) = b(n-2)$. But $b(3) = a(1)$, $b(4) = a(2)$, Hence...

REFERENCES

APPEL, K. and HAKEN, W. "The Solution of the four colour map problem." Scientific American, October 1977, pp. 108-121.

AVITAL, S. and HANSEN, R.T. "So simple and so rich: the mailbox principle", Mathematics Teaching. No. 76, September 1976 .

BELL, E.T. Mathematics - Queen and Servant of Science. Bell, 1952.

BLUMENTHAL, L.M. A modern view of geometry. Freeman, 1961.

BOLTYANSKI, V.G. Equivalent and Equidecomposable figures. D.C. Heath, 1963.

COURANT, R. and ROBBINS, H. What is Mathematics? Oxford U.P., N. York 1941.

ESTERMANN, T. "A proof of the irrationality of $\sqrt{2}$." Math. Gaz. 408, June 1975. p. 110.

EVES, H. and NEWSOME, C. Introduction to the foundations and fundamental concepts of mathematics. Holt Rinehart, 1964 .

FETISOV, A.I. Proof in geometry. D.C. Heath, 1963.

FLETCHER, T.J. "Doing without calculus." Math. Gaz. 391. February 1971, pp. 4-17.

FLETCHER, T.J. Linear algebra through its applications. Van Nostrand, 1972 .

GALILEO, G. Dialogue concerning Two New Sciences. Dover, 1954.

HARDY, G.H., LITTLEWOOD, J.E. and POLYA, G. Inequalities. C.U.P., 1934.

HEATH, Sir T.L. The Thirteen Books of Euclid's Elements. Vol. I. Dover, 1926.

HIRST, K.E. and RHODES, F. Conceptual models in mathematics. Allen and Unwin, 1971.

KAC, M. and ULAM, S. Mathematics and Logic. Penguin Books, 1971 .

KLEIN, F. Elementary mathematics from the advanced standpoint. Vols. I and II. Dover, 1939.

LAKATOS, I. Proofs and refutations: the logic of mathematical discovery. C.U.P., 1976.

McCANN, G. "Pythagoras without squares". Mathematics Teaching No. 75. June 1976 .

MAXWELL, E.A. Fallacies in mathematics. C.U.P., 1959 .

MOSES, S. The art of problem solving. Transworld, 1974.

NAGEL, E. and NEWMAN, J.R. Gödel's proof. R.K.P., 1971 .

NORTHROP, E. Riddles in mathematics. Penguin Books, 1944 .

OPEN UNIVERSITY. Logic II - Proof. Mathematics Foundation Course Unit 17. O.U. Press, 1971..

POLYA, G. Induction and analogy in mathematics. Princeton University Press, and Oxford U.P., 1954.

POLYA, G. Mathematical discovery. Vols. I and II. Wiley, 1963, 1965..

POPP, W. History of Mathematics. Topics for schools. Transworld, 1974.

REICHMANN, W.J. The Spell of Mathematics. Penguin, 1972 .

REID, C. From zero to infinity. Routledge, 1968.

SAWYER, W.W. Prelude to Mathematics. Penguin, 1955 .

SCHOOL MATHEMATICS PROJECT. Advanced Mathematics IV. C.U.P., 1968 .

SIERPINSKI, W. A selection of problems in the theory of numbers. Pergamon, 1964.

SKEMP, R.R. The psychology of learning Mathematics. Penguin, 1971 .

SOMINSKII, I.S. The method of mathematical induction. D.C. Heath and Co., 1963 .

STEWART, I. Concepts of modern mathematics. Penguin, 1975 .

STOLL, R.R. Sets, logic and axiomatic theories. Freeman, 1961..

TRAKHTENBROT, B.A. Algorithms and automatic computing machines. D.C. Heath 1963 .

WALKER, R. "The pigeonhole principle". Mathematical Gazette, No. 415, March 1977 .

WHEELER, D.H "Genesis of a problem." Mathematics Teaching 82. March 1978, pp. 50-51.

WHEELER, D.H. R is for Real. Open University Press, 1974 .

WOODALL, D.R. "Inductio ad absurdum." Math. Gaz. 408. June 1975, pp. 64-70.

INDEX

INDEX OF SYMBOLS

INDEX OF PROBLEMS