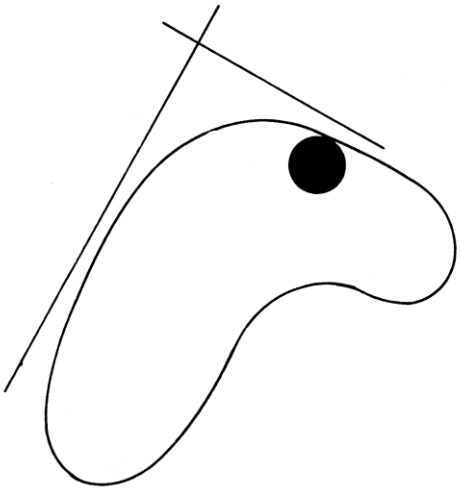


M500 51

M500 is a student-owned, student-operated magazine for Open University mathematics students, staff and friends. It is designed to alleviate student academic isolation by providing a forum for public discussion of the mathematical interests of members.

Articles and solutions are not necessarily correct but invite criticism and comment. Anything submitted for publication of more than about 600 words will probably be split into instalments.

MOUTHS is a list of names and addresses, with telephone numbers and details of past and present courses of voluntary members, by means of which private contacts can be made to share OU and general mathematical interests - or to form self-help groups by telephone or correspondence.

MATES is a special list of MOUTHS members who have explicitly volunteered for their MOUTHS details to be distributed to members in closed institutions such as prisons and special hospitals.

The views and mathematical abilities expressed in M500 are those of the authors and may not represent those of either the Editor or the Open University.

::

PUBLISHER Marion Stubbs cover designs, missing issues, missing pages

EDITOR Eddie Kent articles and letters for publication

PROBLEMS EDITOR Jeremy Humphries problems and solutions for publication

MEMBERSHIP SECRETARY Joyce Moore subscriptions, changes of address, MOUTHS/MATES data

TREASURER Austen F. Jones, ACA

WEEKEND ORGANISER 1978 Sidney Silverstone

PRINTER - Waterside Printing Company, Southampton

M500 51 published April 1978. Subscription £4 for 10 issues. Cheques and postal orders should be payable to THE M500 SOCIETY, crossed "ACCOUNT PAYEE ONLY. NOT NEGOTIABLE" for safety in the post.

ANYTHING SENT TO ANY OFFICER OF THE SOCIETY WILL BE CONSIDERED FOR POSSIBLE PUBLICATION IN THE MAGAZINE UNLESS OTHERWISE SPECIFIED.

::

The cover design is by Bob Greig and is called "Portrait of a Neighbourly Subset"

THE DELIMITER GAME

JOHN JAWORSKI

Suppose that I handed you a card, face downwards. I now ask you to look at the other side of the card and tell me what you read on it. On the surface this presents no major problems. However, the situation is a very deep one and, as I shall show you in a moment, unless you make some crucial decisions, and communicate those decisions to me before you turn the card over, the situation is an impossible one.

To illustrate the difficulties, let us suppose that the first card (there will be more!!) is completely blank.

Quite reasonably, you will probably reply, 'Nothing'.

I choose to make my point in a rather more subtle way - I silently hand you another card. This time when you turn it over you discover written on it, 'NOTHING'.

In ordinary speech we may continue. Probably you reply, 'This card has the word "nothing" written on it'.

Fair enough. Except that my card following that card bears on it, 'THIS CARD HAS THE WORD "NOTHING" WRITTEN ON IT'.

Clearly from now on, and indeed from the time you looked at the first card the situation is hopeless: whatever you wish to say to me might well turn up on the card following. You are no longer capable of distinguishing to my satisfaction between the text on the card and the instructions that you wish to give to me about the manner of your relaying the text.

A lot of observations can be made; one is that we do circumvent this problem in everyday speech, and even the most pedantic philosopher would probably be convinced by inferences drawn from inflections of the voice, deliberate pausing and so on. Indeed we may very well reason that the problem is a highly artificial one that never occurs in practice.

Let me answer both of these points. Clearly I could construct some restrictions on the original problem, such as requiring you to answer only by telegram or through a typewriter, &c, which would retain the essence of the problem without allowing you the immediate short cuts of speech.

Further, the problem has arisen in practice! It occurs most frequently in computing where the present state of the art causes us to spend a lot of time using computer instructions to process computer instructions. Using language to talk about language is far from uncommon. Furthermore, most of the restrictions about the tone of the respondent's voice are automatically imposed as soon as the problem is set in a computing context.

The problem, stated as concisely as possible, is: *How do we transmit a message of arbitrary content, remembering that* delimiters *such as a signal to indicate the end of the message mau properly be part of the message*?

One attractive solution but with a flaw is to say that I shall tell you what is on each card within (say) five seconds. The flaw can be demonstrated by constructing a message so long that it cannot ➔

be transmitted in whatever time limit you impose. However long you choose there is always a message that is longer; but this method does indicate that the solution must be agreed between the transmitter and the receiver before the transmission begins. As soon as we could be talking about the contents then it is too late.

The traditional computing solution is to define a character (usually the quote mark ") as a delimiter. In essence we then transmit by

saying 'I shall surround the contents of this card by "... ..." and then transmit the new extended message.' Our cards then become during transmission

1. " "
2. "NOTHING"

and so on.

This solution is theoretically useful but presumes that we can recognise a complete message when we see one. As we, and computers, read left-to-right there are certain problems in sending the message " " " - that is, a message consisting of the quote sign. One way, often adopted, is to take the sign " out of our list of allowable text characters. Unfortunately we shall often want to transmit this character just because it does have this use. An alternative is to choose any message-character that does not appear in the message that we wish to transmit. The computer, and ourselves, recognise the first character of the message as being separate from the message, but informing us that the next occurrence of this character indicates the end of the message. Our cards might well become

1. " " or ** or even AA
2. "NOTHING" or *NOTHING* or XNOTHINGX .

Again, agreement between the participants is required *before* transmission begins. And again, although this is a theoretical rather than a practical objection, I cannot send a message consisting of all the allowable characters. Restricting ourselves to letters and spaces only we cannot for example send

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

except as, perhaps,

XTHE QUICKX

followed by

QBROWN FOX ...Q.

The problem is deeper than it looks.

::

It ... seems that Einstein was doubly wrong when he said "God does not play dice". Consideration of particle emission from black holes would seem to suggest that God not only plays dice but sometimes throws them where they cannot be seen.

S W Hawking *The quantum mechanics of black holes*

BOOKS JOHN HAMPTON

I like Norman Lee's suggestion (M500 48 3) of having a 'For the library' column very much indeed. However, much as I should like to, with M231/M331 on top of me I simply have no time to write much about the many mathematics books I have really enjoyed. So en passant here are some I have used recently and found appealing. I think each is well worth a glance and hopefully many other people will find them useful too. My own favourites are those by Fike, Halmos and Stewart. Happy reading!

Apostol , T M *Calculus I*: *One-variable Calculus with an Introduction to Linear Algebra.* 2nd edition, 666pp, Xerox College Publishing Lexington, 1967. ISBN 0-536-00006-9.

This is a really splendid, very readable, almost classic exposition of calculus which introduces integration before differentiation. I used it extensively as background reading whilst taking M100 and it helped me immensely. More recently I have been using it as gentle preparation for M231. Highly recommended.

Baumann, R; M Feliciano; F L Bauer; K Samelson *Introduction to Algol* l42pp Prentice-Hall Englewood Cliffs, 1964. Lib of Cong Cat Card 64-10740.

Of all the high-level computer programming languages I have used Algol 60 is the one I most highly praise: it is absolutely beautiful and ideal for much numerical computation. This particular book is the best I have seen as a general primer on the language and I use it with my students at the University of Lancaster. The 'Revised Report on the Algorithmic Language Algol 60', which is studied in M251, is given as an Appendix.

Fike, C T *Computer Evolution of Mathematical Functions* 227pp, Prentice-Hall EC, 1968, Lib of Cong CC 68-9142.

A really fabulous book which I started to read having studied the Approximation Theory Units in M201. A good starting point I think if research in function evaluation methods appeals to you.

Gourlay, A R; G A Watson *Computational Methods for Matrix Eigeproblems* 132pp, John Wiley London, 1973, ISBN 0-1471-31915-5.

Another follow-up to M201. A very nice introduction to the eigenvalue/eigenvector problems of numerical linear algebra.

Halmos, P R *Finite-dimensional Vector Spaces* 200pp, Springer-Verlag NY, 197A, ISBN 0-387-90093-4.

I used this classic as background reading to M201 and in particular to supplement Nering. I think it is a wonderful book which should be read by everyone who studies linear algebra. Very highly recommended.

Kirch, A M *Elementally Number Theory*. *A Computer Approach* 339pp, Intext Educational Publishers NY, 1974, ISBN 0-7002-2456-4

If computing is your scene and/or number theory interests you I think that this book is a must. Great fun and highly recommended.

Monro, D M *Interactive Computing with* BASIC; *a first course*. 148 pp, Edward ➔

Arnold, London 1974. ISBN 0-7131-2488-1

Simply the best book I have ever seen on BASIC and having a strong mathematical bias. Again I use it with my students at Lancaster. If Gaussian Elimination has ever worried you read pp 89-95 and study figure 8.4 on page 92: it is a beauty.

Rektorys K (Ed) *Survey of Applicable Mathematics* I369pp, Iliffe Books, London, 1969 ISBN 0-592-03927-7.

An encyclopaedic survey of almost every area of applicable (as distinct from applied) mathematics one can think of, which I dip into whenever I am stuck, need to look something up quickly, simply want to browse, or feel depressed. So far it has never let me down and I referred to it at times during M100, M201 (particularly) and M202. Last year I used it to solve an M231 TMA question for a friend who was stuck. Very highly recommended for browsing and anti-depressive therapy!

Stewart I *Galois Theory* 26pp, Chapman Hall, London, 1973: ISBN 0-412-10800-3.

I used this as background and further reading for M202 Units 31-34. It is a really beautiful book, well written and full of intellectual delights. An absolute must if your interests are in pure mathematics.

* * * * * *

PETER WEIR

Use of Mathematical Literature. Edited by A R Dorling, 260pp, Butterworth, £12 (!!): ISBN 0 408 70913 8

This is the latest book in the series Information Sources for Research and Development, to quote the back cover. That is near the truth, the title being misleading. The book gives details of mathematical information sources: societies, journals, dictionaries, etc, and books. The coverage is very patchy -applied maths is deemed not to exist apart from mathematical programming. Analysis, too, is ignored, as is linear maths.

The topics that are covered are not covered to a uniform degree. This is due to the rise of specialist authors and poor editorial control. Due to my restricted knowledge I can only make a few criticisms. Knuth, an accepted pillar of wisdom, does not get a mention in the Mathematical Programming chapter. Our friend Halmos from M202 is not referenced in the chapter "Logic and Foundations".

To conclude: Don't buy it unless you are using taxpayers' money. Don't rely on it. By all means use it if there is nothing else. And most of all make sure you have pages 35-38 in your edition - the copy I saw didn't.

The chapter titles are Major organisations and journals, Reference materials, Mathematical education, History of maths* , Combinations, Rings and algebras, Group theory, Measure and probability, Complex analysis and special functions, Convexity, Topology, Mathematical programming, Author and subject index.

*OU gets a plug.

METRICS AND RANK CORRELATION PERCY SILLITTO

A professional violinist could presumably list in order of their technical difficulty the n concerti in his repertoire. His agent should be able to rank (ie list) them in order of their popularity with audiences. How closely do these two rankings accord with each other?

The word 'closely' gives a clue. It suggests defining some kind of 'distance' between permutations of the integers 1,2,... ,n. Each concerto now has associated with it two of these integers; one, v_i say, from the violinist and the other, say a_i, from the agent.

It is obvious that $d = (\sum_{i=1}^{n}(v_i - a_i)^2)^{½}$ is a suitable metric = distance function, since it is the usual distance between pairs $(v_1, v_2, ..., v_n)$, $(a_1, a_2, ..., a_n)$ of points in n-dimensional space. An alternative metric can be defined as follows: put the concerti in the order of the violinist's ranking and let b_j be the rank number accorded by the agent to the jth concerto when considered in this order; for each b_j, j = 1,2,... ,n, count how many of the b's preceding b_j are larger than b_j and find the sum, l, of these counts. For example if the orderings are

v - 1 2 3 4 5 6

a - 3 1 5 2 6 4

then l = 0+1+0+2+0+2 = 5. This is in fact an algorithm for ascertaining the number of 'crossings' on an M202 group card and it follows easily from this that t satisfies the requirements for a metric.

Now having got a metric, sny strictly monotonic function of its values is also a measure of distance and may be more convenient in a particular context (just as plotting on loglog paper may make a relationship more obvious). Also, statisticians like their measures of correlation to have values in [−1,1] and this can be arranged for the above two metrics by defining

(Spearman's coefficient of rank correlation) $r_s = 1–6d^2/(n^3–n)$

(Kendall's coefficient of rank correlation) $r_k = 1–4l/(n^2–n)$.

All this will seem pretty obvious and straightforward, perhaps even banal to those who have taken two or three OU maths courses. However, this simple approach through metrization of spaces of permutations is not used in the standard book on the subject of rank correlation, cited below; and to me at least it makes clearer what underlies Kendall's treatment.

Rank Correlation Methods by M G Kendall, Chas Griffin, 4th edition 1970.

[*Ed - For completeness and comparison I shall calculate the value of d in the example used above. It is* $\sqrt{(4+1+4+4+1+4)} = \sqrt{18} = 4.2$.]

MMMMMMMMMMMMMMMMMMMM

30 000 pigeons were released, fill!ng the air with the flutter of a million wings.

- *Newsreel commentary*.

Correspondingly significant positions are held by the Nested Intervals theorem in real analysis and the Nested Rectangles theorem in complex analysis.

There must be a purely set-theoretic formulation of these ideas which could be invoked for use in any particular mathematical structure, but I have not yet seen such a formulation.

Presumably it might run as follows: Consider

$$S_1 \supseteq S_2 \supseteq S_3 \supseteq \ldots \supseteq S_m \supseteq S_{m+1} \supseteq \ldots$$

where S_1 is an infinite set and there exists a function

$$l\colon \{S_1, S_2, S_3, \ldots, S_m, \ldots\} \to C$$

where $C = \{c\colon c = \#A$ for some set $A\}$ (and $\#A$=c means cardinality of A is c); and

$$l(S_m) = \#S_m$$

and further to this, $\lim_{m\to\infty} l(S_m) = 1$.

We wish to show $\bigcap_{i\in I} S_i = K$ where $K \neq \varnothing$ and K is a singleton set.

We know (Halmos, *Naive set theory* p14) that $S_m \supseteq S_{m+1} \Rightarrow S_m \cap S_{m+1} = S_{m+1}$, which forces the general result $S_1 \supseteq S_2 \supseteq \ldots \supseteq S_m \Rightarrow S_1 \cap S_2 \cap \ldots \cap S_m = S_m$. Thus $\bigcap_{i\in I} S_i$ is a subset of Si, and further to this, $\lim_{m\to\infty} l(S_m) = 1 \Rightarrow$ For every $\varepsilon > 0$ there exists a natural number N such that for all natural numbers m

$$m > N \Rightarrow |S_m - 1| < \varepsilon.$$

This forces the existence of $S_k \in \bigcap_{i\in I} S_i : \#S_k = 1$.

As $\lim_{m\to\infty} l(S_m) = 1$ this S_k with $\# S_k = 1$ is the smallest non-empty subset of $\bigcap_{i\in I} S_i$, and furthermore, any S_n where $n > K$, where $\#S_K = 1$, is such that $S_n = S_K$ (because $S_m \supseteq S_{m+1}$ $\forall m \in I$).

Therefore $\forall n \geq K$, $\bigcap_{n\in P} S_n = S_K$; (P = $\{S_K, S_{K+1}, S_{K+2}, \ldots\}$),

$\therefore \bigcap_{i\in I} S_i = S_K = K$, where $K \neq \varnothing$, and K is a singleton set. QED.

Anybody have any comments on this?

[*With regard to Alan Gurr's letter in* M500 49 *where he suggested there should be an* 'M302' *course, I have written to Walton Hall and been told that a* 3*rd level course, provisionally 'Aspects of Abstract Algebra' is being produced and will appear in* 1980/1; *so start expressing interest*!]

GAUSS V JEREMY GRAY

In episode three I described the law of quadratic reciprocity, which stated that if p and q are primes not both of the form $4n + 3$ then p is a quadratic residue mod 1 if and only if q is a residue mod p, but if p and q are both of the form $4n+3$ the reverse is the case. I hope in this episode to describe Gauss's second proof of this theorem, to which a good part of his *Disquisitiones Arithmeticæ* is devoted, because it well illustrates Gauss's belief in the essential unity of mathematics. It was to be of immense significance for algebra, and connected in Gauss's mind with complex function theory, but it starts with a study of two geometric objects: quadratic forms and lattices. (In what follows a couple of sheets of squared paper might come in handy.)

A quadratic form is an expression of the form $ax^2 + 2bxy + cy^2$. What values does it take if a, b and c are fixed integers and x and y variable integers? Which quadratic forms can take the value 1, for instance? We say the quadratic represents A iff $A = ax^2 + 2bxy + cy^2$.

Suppose we have $x^2 + y^2$ in mind. Possible values are $x^2 + y^2 = 0, 1, 2, 3, 5, 8, \ldots$, the numbers which are sums of squares. The points with integer coordinates on the Cartesian plane, (m,n) say are $\sqrt{m^2 + n^2}$ from the origin, so to see if $x^2 + y^2$ represents A draw the circle centre the origin and radius $\sqrt{A}$. If it passes through any points (m,n) the answer is yes, otherwise no.

Suppose we have $x^2 + 4xy + 5y^2$ in mind. The lattice of integer-points will not help us now. Build a lattice by going $\sqrt{a} = 1$ unit from an agreed origin in one direction and $\sqrt{5} = c$ units in a direction inclined at ϕ to the first where $\cos\phi = b/\sqrt{ac} = 2/\sqrt{5}$ ie from the origin to $\left(\frac{\sqrt{D}}{\sqrt{a}}, \frac{b}{\sqrt{a}}\right)$. This gives you a parallelogram. Use it as a tile to build a lattice.

Now the same geometric method applies: A is representable by $x^2 + 4xy + 5y^2$ iff a circle of radius $\sqrt{A}$ and centre the origin ➔

meets a point of the lattice.

You will have noticed that if ϕ is to exist $\left|\frac{b}{\sqrt{ac}}\right| \geq 1$ or $b^2/ac \geq 1$; ie $b^2 - ac < 0$. This makes the quadratic form positive definite (in modern terminology), it cannot represent negative numbers. It turns out that $b^2 - ac$ plays an important role in what follows, so we call it $-D$, for a positive D. Indeed it is easy to see the area of the parallelogram just described is $\sqrt{D} = \sqrt{(ac - b^2)}$, for area = "$\mathbf{x}$–$\mathbf{y}$ sinϕ" = $\sqrt{a}\sqrt{c}\frac{\sqrt{D}}{\sqrt{ac}}$.

In order to simplify the problem we look next for a new lattice simpler than the given one, in the sense that $x^2 + y^2$, being a sum of squares, is simpler than $x^2 + 4xy + 5y^2$. We transform our lattice by introducing

$x' = \alpha x + \beta y$

where $\alpha\delta - \beta\gamma = 1$

$y' = \gamma x + \delta y$

and α, β, γ and δ are integers

The new lattice has a fundamental parallelogram equal in area to the old one: $\sqrt{D}$. We say any two lattices are equivalent if, and only if, they are related in this way. They then define the same sets of points in the plane, but with different bases, that is, the fundamental parallelogram is different in each case. If one of these parallelograms, furthermore, can be a rectangle - α, β, γ, δ, chosen aright - the lattice is then called reduced.

The associated quadratic form is now $x'^2 + Dy'^2$. The chief object of study for Gauss was equivalence classes of lattices under the above equivalence relation! This is a little staggering to contemplate, but you may take consolation from the thought that this is the first time an object in mathematics was studied other than a real number or a function of same.

Thus $x^2 + y^2$ and $x^2 + 4xy + 5y^2$ are equivalent. How does $x^2 + 4xy + 5y^2$ represent 2? From the graphical representation it turns out that $x = -1$, $y = +1$ represents 2. We can confirm the equivalence by 'diagonalising' the quadratic form $x^2 + 4xy + 5y^2$. The transformation ➔

$x' = y$

$y' = x + 2y$

sends $x'^2 + y'^2$ into $x^2 + 4xy + 5y^2$, and the lattice point $(x', y') = (1,1)$, which represents 2, into the lattice point $(x, y) = (-1,1)$, which represents 2.

EXERCISE Find the transforms of the points $(x', y') = (\pm 1, \pm 1)$ and check that they also represent 2.

To each quadratic form we have associated the lattice of points it generates. The correspondence is not one–one, and different quadratic forms are said to be equivalent if they generate the same lattice. We may represent the form by a matrix $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ and observe that $ac - b^2$ is the determinant, so no two forms with different D can be equivalent. (Why not?) But nor does the value of D alone uniquely determine the lattice - there can be inequivalent lattices corresponding to the same D. Gauss (*Disq. Arith*. 173) gave this example: $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ both have $D = 5$, but they are not equivalent. To see this suppose (for a contradiction) that they are; say by

$\bar{x} = \alpha x + \beta y$

$\bar{y} = \gamma x + \delta y$ $\qquad \alpha\delta - \beta\gamma = 1,\ \alpha, \beta, \gamma, \delta$ integers.

We should then have $(\alpha^2 + \gamma^2)x^2 + 2(\alpha\beta + \gamma\delta)xy + (\beta^2 + \delta^2)y^2 = 2x^2 + 2xy + 3y^2$, which cannot be done. So Gauss divided those forms with the same value of $-D$ into genera as we now discuss.

Look at this example more closely. Denote $x^2 + 5y^2$ by f and $2x^2 + 2xy + 3y^2$ by f'. The lattice of points generated by f is found by taking as fundamental parallelogram the tile spanned by the vectors (1,0) and $(0, \sqrt{5})$½. The lattice generated by f' is spanned by the vectors $(\sqrt{2},0)$ and $\left(\frac{\sqrt{D}}{\sqrt{a}}, \frac{b}{\sqrt{a}}\right) = \left(\frac{\sqrt{5}}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right)$. Consider the points representable by f. They include 0, 1, 4, 5, 6, 9, 14, 16, ... The points representable by f' include 0, 2, 3, 7, 8, 12, 15, ... Strike out the multiples of D=5 in each case and reduce, mod D, and you get

f: 1, 4, 1, 4, 1, 4, ... , ➔

f ‘: 2, 3, 2, 3, 2,... .

Those in the first case are always quadratic residues mod 5 whereas this is never true in the second case, and this illustrates a general theorem Gauss was able to prove which given *D* he called the genera.

Gauss then did something quite remarkably new. He observed the forms of the same class can be multiplied together to yield a new form of the same class or, as we should say now: the genera of a given class form a group - an abelian group as it turns out. But this is only 1799, some considerable time before there is any theory of groups (although a theory of permutations is 'in the air'). The definition is somewhat artificial, and in any case this is not meant to be a course in number theory - although you might have begun to suspect otherwise. The point is rather to indicate the importance of Gauss's second proof of the law of quadratic reciprocity for the development of algebra. So we must reintroduce the quadratic residues. It is evident from our example that they determine the genera of forms with a given *D*. The group law is therefore some kind cf an equation between the genera or, equivalently, between the residue classes that determine the genera - unravel the equation and you have the law cf quadratic reciprocity.

It's a long journey from lattices to groups, quadratic reciprocity and sums cf squares. There was a lot of work needed before Gauss's monumental study cculd be said to be understood by mathematicians. I should like to end with two observations. One concerns a now familiar and crucial trick in the study cf mathematical problems: if you can't solve an equation/problem enlarge the field of enquiry. When Gauss came to invent the law of biquadratic reciprocity (congruences $x^4 \equiv a \bmod p$) he found the statement messy. But if by prime was meant a prime "Gaussian" integer, prime in the ring $\mathbb{Z}[i] = \{p + q \in \mathbb{Z}, i^2 = -1\}$ it became easier. So, to study integers don't stay in $\mathbb{Z}$, go up to $\mathbb{Z}[i]$, work there and then come back to $\mathbb{Z}$.

My second observation concerns this adjoining of ideal elements, such as *i*, to a ring (or a geometry, or ...) but specifically to a ring like $\mathbb{Z}$ or a field like $\mathbb{Q}$. It is the start cf algebraic number theory. Is factorization unique? Yes in $\mathbb{Z}[i]$, no in $\mathbb{Z}[5i]$. Very well, add more elements in $\mathbb{Z}[5i]$ until factorization is unique again. These are Kummer's ideal elements (1847) later reorganized into ideals by Dedekind (1871) and independantly by Kronecker.

ADVERTISMENT OR CRY FROM THE HEART JOYCE SMITH

Has anyone seen, or borrowed, MST282 units? A line or phone call would be appreciated. Also, I have a spare set of M331 units and broadcast notes (unmarked) if anyone wants them for £5 (plus postage).

Ed - Joyce says if she gets the five pounds one of them will go to the M500 *equipment fund; and that to advertise in Sesame costs* £1 *and seems hardly worth it. It seems worth pointing out again that members can advertise free in* M500 *since the magazine is the property of THE M500 SOCIETY which is nothing if not its members. I remember that someone tried selling a car through its pages once, though I don't know with what success.*

TV IN THE MATHEMATICS CLASSROOM COLIN MILLS

I have received a notice of an IMA (Institute of Mathematics and its Applications) meeting which might be of interest.

It is a one day course for teachers on the use of Open University mathematics television programmes as a teaching resource for fifth and sixth forms and colleges; based on the new M101 programmes. Some programmes will be shown and their relevance to O- and A-level and college mathematics will be discussed. Those attending will take part in small group viewings and discussions to explore ways in which the programmes could be used by teachers as resource material, Amongst others present will be Professor Pengelly.

The fee is £8 ...

The meeting is at Chelsea College London on 6th May 1978.

SOME LETTERS

From Terence Manly The Mathematicians Creed: The good mathematician should at all times keep the aims and objective of his problem clearly in view. When dealing with his staff he should state precisely what is required of them and give his orders in such a manner that they can be carried out with the minimum of trouble and supervision. When talking to managerial and administrative staff he should avoid the use of technical speech which could cause ➔

confusion to those who haven't had mathematical training. Remember at all times: you are in charge.

But all of this is difficult to remember when you are up to your neck in alligators, you should have been an engineer anyway and the problem is to drain the swamp.

From; Marion Stubbs There could be a staff 'critic' as well as a small hand-selected batch of student 'critics' for M500. There could even be a regular feature page: What Our Random Sample Of Six Students And One Staff Thought Of M500 $n-1$. Like one or two pithy sentences each, taken down from telephone conversations. Its just an idea. I fancy the editor is much too surrounded by post-graduate types who have no memory of the former ignorance. *They* really need something like *American Mathematical Monthly* to satisfy them. Kaybe they ought to start up OPEN SET or even M1000. I wanted such a thing years ago and was trying to get the staff to produce one, maybe quarterly, but they would not. These superior critics are all very good at criticising but don't seem to write anything themselves, apart from our stalwart team of Staff-MOUTHS who do their stuff in M500.

From Jeremy Humphries Just got 49: What do you mean "James R Newman who's he??" (Two question marks!)

But for him you would not have a Problems Editor. I began to realise that not all maths was like what I was taught at school, and some of it right be inteesting, only on reading *Mathematics and the Imagination* by Edward Kasner and James Newman.

My brain cells are going exponentially too, but I think it was Kasner who asked his grandson (nephew?) for a name fcr 10^{100} and received GOOGOL. I have just been caught by a colleague at work who was pretending to do a crossword and asked for help with a clue: 'Overloaded postman'. Of course I replied "How many letters?"

From EK I suppose this isn't a real letter but you wouldn't really want me to waste a sevenpenny stamp, would you?

Those who didn't bother to come to the Weekend 1977 missed, among other things, Graham Read's story of the fly and the locomotive. I hope he doesn't mind if I reproduce it here since it is well worth considering (and anyway one would like the opportunity of thanking Graham for stepping into a breach at short notice).

The story depends on the Intermediate Value Theorem which states in part that if a continuous function has a negative and a positive value there is a point in between where its value is zero.

$$(f(a) < 0, f(b) > 0 \Rightarrow \exists x \in (a,b) \text{ such that } f(x) = 0.)$$

There is a locomotive puffing along its track at 60mph. Travelling directly towards it on the same line is a fly, doing 5mph. There comes the fly's moment of glory: they collide!

Consider: At some time the fly was travelling at 5mph in one direction; later it was doing 60mph in the opposite direction. So, by our theorem, at some time it was stationary. But at that moment it was plastered over the windscreen of the train. Therefore the train was also stationary. So in its one brief moment of extasy our fly stopped the Coronation Scott.

SOME THOUGHTS ON "LINEAR DIFFERENCE" (M500 44 1) PETER HARTLEY

1. What's a 'discrete variable'? Isn't y_n a value of a function of a discrete variable (n)? Does that make y_n a discrete variable? $y = f(x)$ where $x \in$ 'continuous domain' in $\mathbb{R}$ doesn't make y 'continuous' necessarily.

2. Why use y_n but $\phi(n)$ since y is also a function of n?

3. Why 'particular integral' not 'particular sum'? I ask this because the recurrence relation (as I call it)

$$y_{n+r} + a_1 y_{n+r-1} + \ldots + a_r y_n = \phi(n)$$

can be written as a (proper) difference equation

$$\Delta^r y_n + b_1 \Delta^{r-1} y_n + \ldots + b_r y_n = \phi(n)$$

and difference equations are solved essentially by summation not integration (though admittedly sometimes called 'discrete integration!') For example

$$y' = f(x,y) \qquad , \qquad x \geq 0$$

leads to the implicitly stated solution

$$y(x) = y(0) + \int_0^x f\big(t, y(t)\big)dt$$

and

$$\Delta y_n = f(n, y_n) \qquad , \qquad n \in \mathbb{Z}^+$$

leads to

$$y_n = y_0 + \sum_{i=0}^{n-1} f(i, y_i)$$

4. Is Richard Shreeve (M500 44) implying that trial and error is the only method for finding particular 'integrals'? There's a discrete analogue of the Laplace transform called the *z*-transform, and I'm sure we could invent some discrete Green's functions for linear difference operators, although I've not seen that in print. Anyone who's heard of the *D*-operator method for constant coefficient differential equations will not be surprised that there is a discrete analogue.

I think everything above is more a criticism of the mystique and jargon of difference equations - see M201 0711 - than of Richard's piece. I feel that the analogy with differential equations is close enough for the subject to be more easily taught and discussed.

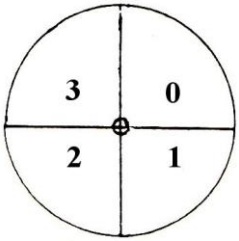
Reference - there is a small amount on diffence equations, and summation as 'anti-differencing' in Scheid, *Numerical Analysis* - McGraw-Hill (Schaum Outline Series).

Ed - Apologies are due for my tardiness in printing this comment on an article that appeared so long ago. If anyone hasn't got issue 44 *and is sincerely interested, write to me and I will get them a copy of* M500 44 1-2.

I have had occasion to read aloud the phrase "E ' where E is any dashed set". It is necessary to place the stress with care.

J E Littlewood

GAFFER'S GAME JOHN HALE



RULES: Throw a stone into the circle. Throw another also. Count clockwise from the first stone by the number of extra positions indicated by the second stone. Remove the first stone, leaving the second in the new position.

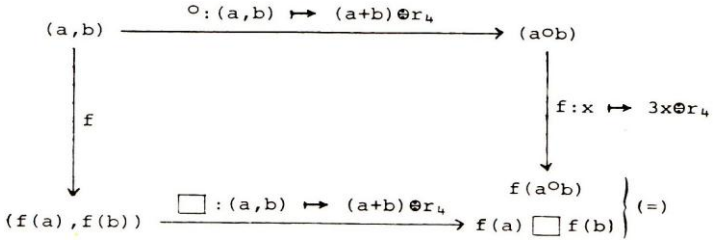
Then, if the second stone is on evens, leave it there, but if on odds transfer it to the opposite side of the circle. (0 counts as even.)

The final position is the score for the first player and the second tries to beat it.

PROBLEM: To represent it in purely mathematical terms by two different formulae.

CLUE: Morphism and distributivity (and clocks?)

ANSWER: With a,b,a°b ∈ {0,1,2,3}



(f is a morphism from ({0,1,2,3},°) to f(({0,1,2,3}),□)).

In fact □ ≡ °, dead easy to eggheads but not perhaps to beginners like me!

Thus clock multiplication is distributive over clock addition.

TEST:

Throw (a)	Throw (b)	a°b	f(a°b)	f(a) □ f(b)	(f(a),f(b))
0	0	0	0	0	0 0
0	1	1	3	3	0 3
0	2	2	2	2	0 2
0	3	3	1	1	0 1
1	0	1	3	3	3 0
1	1	2	2	2	3 3
1	2	3	1	1	3 2
1	3	0	0	0	3 1

. . . .

PROBLEMS CORNER - JEREMY HUMPHRIES

I was pleased to find a couple of new names in the post for this issue. Welcome to all new subscribers. I hope that you will all become contributors.

Of course, we want contributions from everybody, as I frequently say. You all want a magazine and the magazine wants a supply of items. I see that in issue 48 there are about sixteen names mentioned, not counting officers. The membership is 400-500 , so a 'fair share' of contributing would be one communication every 2½ years. That's not a lot, is it?

I've now managed to get a proper look at Martin Gardner's column in November's *Scientific American*, about which I was a little vague in 49. This is the article which explains the notation for large numbers invented by Donald Knuth. The article is about graph theory, specifically Ramsey Theory, and anybody interested in graphs ought to have a look at it. The big number which comes into it really is big. Perhaps it will become famous as Graham's Number. (cf the miniscule Skewes.)

But what is a big number? The number of pound notes you would like to find in the street? The number of atoms in the universe? I suppose in one sense there are no big numbers. Choose a positive finite number, say Graham's Number, G. Now choose another arbitrary pfn, say x. It's very unlikely that x is less than G - in fact for a random x the probability x < G is zero. So all numbers are as near zero as makes no difference. QED.

You can see that I'm not very good at inventing names for problems. If you are any better please put a name on any problems you send. And if you've get a solution please send that too.

SOLUTION 48.1 FATHER CHRISTMAS *Father Christmas wants to open his warehouse at noon on Christmas Eve. The door has an electrical lock with* 20 *lights numbered* 1 - 20, *each with its own switch. A switch is inoperative unless the next lower numbered light is on and all the other lower numbered lights are off. Switch* 1 *is always operative. When all the lights are on the door opens. All lights are initially off. The gnomes can perform one operation per second. An operation is turning on or off a light. When must they start opening the lock*?

STEVE AINLEY, LUCY POLAND, MARION STUBBS and SIDNEY SILVERSTONE got this right. This is Lucy:

The number of operations needed to get light n on is 2^{n-1}. This is easily proved by induction. So to get light 20 on needs2^{19} operations. Now light 19 is on so we next must get 18 on. This takes 2^{17} operations. Now 17 is on so 16 comes next, then 14, 12 and so on down to 2. Total number of operations = $2^{19} + 2^{17} + \ldots + 2 = 699050$.

Sidney arrived at the same result after finding general expressions for even and odd n, much the same as Lucy's.

For eve n n, $S(n) = 2^{n-1} + 2^{n-3} + \ldots + 2^{n-(n-3)} + 2^{n-(n-1)}$.

For odd n, $S(n) = 2^{n-1} + 2^{n-3} + \ldots + 2^{n-(n-2)} + 2^{n-n}$.

These can be simplified to $(2^{n+1}-2)/3$ and $(2^{n+1}-1)/3$. The gnomes ➔

take 699050 seconds to open the lock and must therefore start at 9.49.10 am on 16th December. Everybody who didn't get that answer got 200 seconds which is the answer to the question if 'inoperative' is taken to mean simply 'will not turn the light on'. Then for n even $S(n) = n^2/2$ and for n odd $S(n) = (n^2+1)/2$.

In the original problem the rules for operating the switches are equivalent to the rules for generating a cyclic binary or Gray code. Gray codes are used in data handling and have the advantage that successive integer representations differ in only one bit. eg, in standard binary

15 = 01111, 16 = 10000.

In cyclic binary

15 = 01000, 16 = 11000.

To convert cyclic binary to standard binary first take the most significant bit then form successive sums modulo 2 working towards the least significant bit. The standard representation is the listing of the first bit and the successive sums. eg Cyclic 11010. Most significant bit = 1 +1=**0** + 0 = **0** + 1 = **1** + 0 = **1**. Therefore standard is 10011.

To convert from standard to cyclic take the standard number, form another number by dropping the last digit, and add the two numbers modulo 2 without carry. eg 10011 + 01001 = 11010.

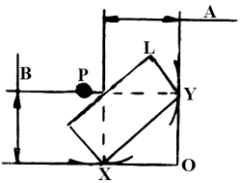
In the problem the lamps start as 000...00 (20 times) and finish as 111...11. Now 111... 11 is simply the number of operations to reach this condition expressed in cyclic binary. (And of course the number of operations to reach any intermediate condition is represented by the sequence of 1's and 0's which matches the on/off state of the lamps.) 111...11 converts, as expected, to 101...010 in standard binary, which is the formula Lucy and Sidney got for n = 20.

Lucy did some investigating of the switching sequence, which begins 1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,5,1,2,1,3,1,2,1,4,1,2,1,3,1,2,1,6,... . If you take a string of zeros numbered 1,2,... from the right and operate on them with this sequence, changing the value (0 or 1) at the position indicated, you will generate the cyclic binary numbers 1 to 32. I'm not going to do it or Eddie will go mad typing it.

Lucy notes that in general in her sequence the 2^nth term and every following 2^{n+1}th term is n +1. (n = 0,1,2,....)

Martin Gardner has an article on Gray codes in *Scientific American* for August 1972. In the same issue there is a piece by F G Heath on origins of the binary code in which Gray codes are also mentioned.

SOLUTION 48.4 RECTANGULAR PLATE *What is the largest rectangular plate which will go round a* 90° *corner in a corridor with arms of width* A *and* B?



This is from BOB ESCOLME:

There are two solutions OYPX and LMXY. Both these rectangles have area AB.

XY = $\sqrt{A^2 + B^2}$. LY = AB /$\sqrt{A^2 + B^2}$. The two arcs centre P radii PX and PY indicate that LMXY will pivot instantaneously about P, just glancing the inner walls. The semi circles YLP and PMX are of no real significance but ➔

they are useful in showing that there are no other solutions.

Others who got this result are BOB BERTUELLO and STEVE AINLEY who proposed the problem. Steve in fact sent a long rigorous proof which confirmed Bob's intuitive solution.

PROBLEM 51.1 POWERFUL DIGITS JOHN HULBERT

There are just two four-digit numbers, x and y, which have the property that they are equal to the sum of the fifth powers of their digits. Given that $y = x+1$, find x and y.

John is one of the new names and is 'full of enthusiasm' which is good to hear.

I find properties like that described very interesting. Let's call this one $(4)5$. Does anyone feel like trying to find some more? There is only one $(4)^4$ that I have found. An example each of $(6)^5$ and $(8)^8$ were printed in issue 49. Who can find the most impressive $(a)^b$? Obviously these are computer jobs but if anyone wants to go on searching I am, as I say, interested.

PROBLEM 51.2 AGES

When my sister is four times as old as she was when I was twice as old as she was when I was twice as old as my brother, my brother will be two-thirds as old as I will be. My brother and I are teenagers; how old was my sister on her last birthday?

PROBLEM 51.3 ROOTS JOHN HULBERT (again)

It is well-known that if

$a_n = a_{n-1} + b_{n-1}$

$b_n = a_{n-1} + a_n$

then $\lim_{n\to\infty} b_n/a_n = \sqrt{2}$.

Generalise to find the mth root of any positive integer.

PROBLEM 51.4 DIVISION BY SIX PERCY SILLITO

Percy says: I found this simple problem in the course of some work recently. Since there is a demand for easy problems in M500 it may be suitable.

Show that if j is an integer >1 then $t = (2j-1)j(j-1)$ is divisible by 6.

PROBLEM 51.5 MULTIPLICATION KRYSIA BRODA

Prove that $\prod_{0\le i<j\le n} \frac{a_i - a_j}{i-j}$ is an integer, where a_0, ..., a_n are $n+1$ *positive* integers. (If any of $a_0,\ldots,a_n$ is zero the result obviously holds.)

EDITORIAL

First of all, there was an **ERROR** in M500 49 2. It was pointed out by Timothy Wilkins (MATES) and confirmed by Jeremy Gray: In *Gauss* IV, G3. should read "area ... is *proportional* to $\alpha + \beta + \gamma - \pi$".

Secondly, two points from the Problems Section; Jeremy says no solutions at were offered to SCRAMBLE; if this goes on he will use his own solution next month. And TWO QUITE DIFFERENT solutions have come for MODULUS: 48.2 *If* $|x| < 0.1$ *and* $y < 0.1$ *what is the probability that* $|x - y| < |xy|$? THURSTON HEATON says 0.05 and MICHAEL GREGORY says 0.031 . Who is right? or are they different ways of looking at the same problem. If no reply comes to this full details will be given in our next.

Since Gődel died recently it is natural to think about his, some say, greatest achievement. Any set of axioms must be consistent - that is, it must be impossible to deduce a theorem and its converse (-(a∧-a)) from them. Also it is pleasant if the axioms are complete, ie Any theorem which is true in the system should he deducible from the axioms.

Let us take arithmetic. Set up a one–one matching from formulæ in arithmetic to statements about arithmetic such that every deducible formula corresponds to a true statement.

Gődel constructed a formula, G, which corresponded to the statement "The formula G cannot be deduced from the axioms".

If G can be deduced from the axioms then its statement is false, hence not all deducible formulæ correspond to true statements; this is a contradiction. Therefore G cannot be deduced. Suppose then, that the converse of G can be deduced. The statement corresponding to the converse of G is the converse of the statement corresponding to G (clearly!!) That is "The formula G can be deduced from the axioms". Since formulæ correspond to true statements, this is true; there is no contradiction this time. So we now have the situation where both G and its converse can be deduced, and either the axioms are not consistent, which is not allowed, or neither G nor its converse can be deduced from the axioms. It follows, once you have constructed G that the system, is either incomplete or inconsistent.

Let us, I hear you say, use this remarkable fact on a concrete example. Let us test Goldbach's Conjecture: Every even number is the sum of two primes. Suppose this is wrong - then there exists some even number which is in no way a sum of two primes. Since this number exists it can be found, in theory at any rate. So the conjecture is decidable. If, on the other hand, it is undecidable this can only be because no such number exists: hence the conjecture is true. That is, any proof that, the conjecture is undecidabie is a proof that it is true, and therefore decidable.

Is this a contradiction?

A new prime has been discovered. It is the number 111, 1...1, 111 (317 ones). Any number made up entirely of ones like this is called 'repunit'. R_n is defined as $(10^n - 1)/9$, so the number of ones in R_n is n. R_n prime $\Rightarrow$ n prime, but the implication is not reversible except in the case of n = 2, 19, 23 and now 317. The proof of primality is by Hugh C Williams of the University Manitoba using a technique of finding sufficient factors of $R_{317}-1$.

My information comes from *Scientific American*, February. The next possibility for R_n prime is n = 1031.

Eddie Kent