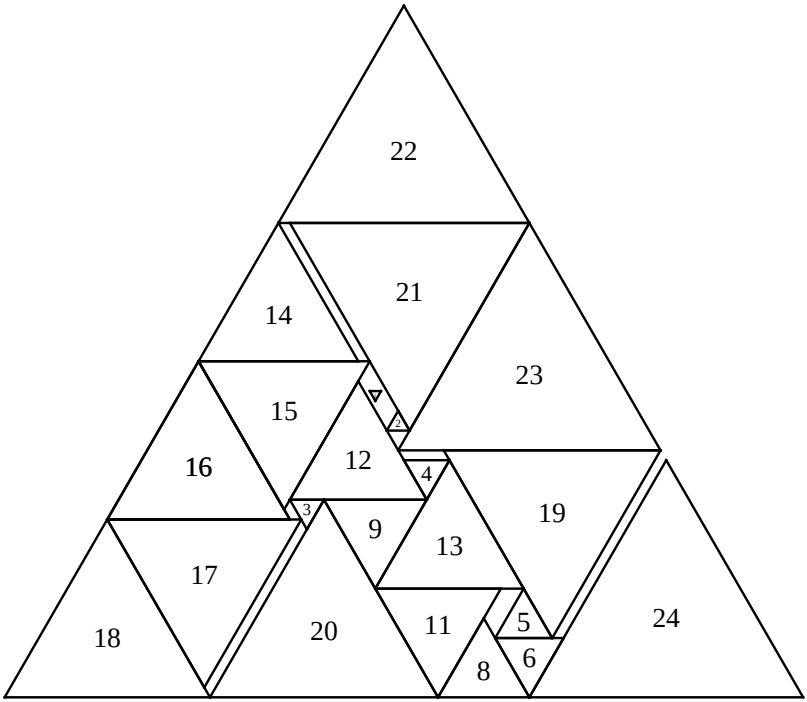
*

ISSN 1350-8539

M500 182



The M500 Society and Officers

The M500 Society is a mathematical society for students, staff and friends of the Open University. By publishing M500 and 'MOUTHS', and by organizing residential weekends, the Society aims to promote a better understanding of mathematics, its applications and its teaching.

The magazine M500 is published by the M500 Society six times a year. It provides a forum for its readers' mathematical interests. Neither the editors nor the Open University necessarily agree with the contents.

MOUTHS is 'Mathematics Open University Telephone Help Scheme', a directory of M500 members who are willing to provide mathematical assistance to other members.

The September Weekend is a residential Friday to Sunday event held each September for revision and exam preparation. Details available from March onwards. Send SAE to Jeremy Humphries, below.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. Send SAE for details to Norma Rosier, below.

Advice to authors. We welcome contributions to M500 on virtually anything related to mathematics and at any level from trivia to serious research. Please send material for publication to Tony Forbes, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation. If you use a computer, please also send the file on a PC diskette or via e-mail. Camera-ready copy can be accepted if it follows the general format of the magazine.

Recurrence Relations

Dave Turtle

We begin with an outline of an analytic proof that the recurrence relation

$$U_n \;=\; \frac{1}{k}(U_{n-1} + U_{n-2} + \cdots + U_{n-k})$$

converges to a limit, followed by a method of calculating the limit directly from any consecutive sequence of k terms.

Consider the set $S(n) = \{U_{n-x} : x \in \{1, 2, \ldots, k\}\}$, the set of k consecutive terms preceding U_n. Since U_n is equal to the mean of the terms in this set, by the rule of the recurrence relation, either all the terms in the set are equal (in which case we already have convergence), or

$$U_n \;>\; \min S(n), \tag{1}$$
$$U_n \;<\; \max S(n). \tag{2}$$

Thus

$$\min S(n+1) \;\geq\; \min S(n)$$

and

$$\max S(n+1) \;\leq\; \max S(n).$$

Furthermore, after at most k steps in the sequence both $\min S(n)$ and $\max S(n)$ will have dropped out of the set and the elements added to the set will be strictly greater than $\min S(n)$, by (1), and strictly less than $\max S(n)$, by (2); that is,

$$\min S(n+k) \;>\; \min S(n),$$

$$\max S(n+k) \;<\; \max S(n).$$

The sequence $A(n) = \min S(kn)$ is therefore strictly increasing and the sequence $B(n) = \max S(kn)$ is strictly decreasing. Clearly, $A(n) < B(n)$ for all n so both sequences converge (by the axiom of completeness for the real numbers)—the only question is whether they converge to the same limit. If they do then the conditions (1) and (2) mean that U_n will be squeezed between these two sequences and will thus converge to the same limit.

Suppose they converged to different limits, $A(n) \to a$, $B(n) \to b$; then for any d we can find some N_a such that $|A(n) - a| < d$ for all $n > N_a$, and similarly N_b such that $|B(n) - b| < d$ for all $n > N_b$. Choose $d = (b-a)/(4k)$ and let $N = \max\{N_a, N_b\}$. Now for $n > N$ we have $|A(n) - a| < (b-a)/(4k)$

and $|B(n)-b| < (b-a)/(4k)$, but all the new terms added to the set $S(kn)$ will be in the range $(a+(b-a)/(4k),\ b-(b-a)/(4k))$ since, in the worst case, we will have either

1. only a single term equal to $a+(b-a)/(4k)$ and $(k-1)$ terms equal to $b+(b-a)/(4k)$, or

2. one term equal to $b-(b-a)/(4k)$ and $(k-1)$ terms equal to $a-(b-a)/(4k)$.

In case 1 U_{kn} will be

$$\begin{aligned}\frac{1}{k}\left(a+(k-1)b+k\frac{b-a}{4k}\right) &= b+\frac{b-a}{4k}-\frac{b-a}{k}\\ &= b-3\frac{b-a}{4k} < b-\frac{b-a}{4k}.\end{aligned}$$

Also $U_{kn} = a+(b-a)(1-3/(4k) > a+(b-a)/(4k)$ since $b > a$ and $1-3/(4k) \geq 1/(4k)$ for $k \geq 1$. Case 2 is just the mirror image of this.

This all means that after at most k steps of the recurrence relation we will no longer have any terms at all within d of either a or b, so neither $A(n+1) = \min S(k(n+1))$ nor $B(n+1) = \max S(k(n+1))$ will be in the required ranges, contradicting the supposition that $A(n)$ and $B(n)$ converge to these limits.

To calculate the limit, start by considering the expression

$$T(n) = \sum_{m=1}^{k} mU_{n-k+m-1};$$

for example, for $k=3$, $T(5) = U_2+2U_3+3U_4$, so

$$T(n+1) = T(n)-(U_{n-k}+U_{n-k+1}+\cdots+U_{n-1})+kU_n.$$

But $kU_n = U_{n-k}+U_{n-k+1}+\cdots+U_{n-1}$ by the rule of the recurrence relation; so $T(n+1) = T(n)$ for all n. Call this constant t.

From the proof that U_n converges we know we will eventually obtain a sequence of k terms which are all within $\pm d$ for any d, however small, and T for this sequence, call it $T(N)$, will still be equal to t, the T value for the sequence we started with. If u is the limit of U_n then $T(N)$ will be equal to $k(k+1)u/2$ plus or minus some error term whose value will be less than $k(k+1)d/2$. Since we can choose d to be as small as we wish it must be the case that

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

So

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

that is,

$$u \;=\; \frac{2}{k(k+1)} \sum_{m=1}^{k} mU_{n+m},$$

where n is anything we like.

This also explains why 3, 6, 10 and 15 turned up as divisors where they did, since $3 = 1 + 2$, $6 = 1 + 2 + 3$, $10 = 1 + 2 + 3 + 4$, $15 = 1 + 2 + 3 + 4 + 5$, ...

Weighted means

This method generalizes to any recurrence relation of the form

$$U_n \;=\; \sum_{m=1}^{k} C_m U_{n-m},$$

where $\sum_{m=1}^{k} C_m = 1$ and each $1 > C_m > 0$; that is, where the next term is any kind of 'weighted mean' of the k preceding terms.

The C_m values must be less than one and strictly positive to preserve the conditions for the convergence proof that $U_n > \min S(n)$ and $U_n < \max S(n)$. With negative or zero C_m values we can still get $T(n+1) = T(n)$ but the sequence may cycle. For example, suppose

$$U_n \;=\; U_{n-1} - U_{n-2} + U_{n-3};$$

then if $U_0 = 5$, $U_1 = 7$ and $U_2 = 11$, we get $T(n) = 16$ for all n but the sequence is periodic:

$$U_n \;=\; 5,\ 7,\ 11,\ 9,\ 5,\ 7,\ 11,\ 9,\ \ldots.$$

The choice of d in the proof that A and B converge to the same limit must be modified to $d = C_\mu(b-a)/(4k)$, where C_μ is the minimum of the C_m, since in case 1 we will have one term of weight C_μ equal to $a + d$ and weights summing to $1 - C_\mu$ at $b + d$. The modification is similar for case 2.

To calculate the value to which the sequence converges just put

$$T(n) \;=\; \sum_{m=1}^{k} D_m U_{n-m}$$

with $D_1 = 1$, then solve $T(n+1) = T(n)$, equating values of U_x and expanding U_n using the recurrence relation, to obtain k simultaneous equations in the terms C_m and D_m. It turns out that the D_ms are given by

$$D_m = \sum_{x=m}^{k} C_x;$$

e.g. for $k = 3$, $D_3 = C_3$, $D_2 = C_3 + C_2$ and $D_1 = C_3 + C_2 + C_1 = 1$. Thus U_n converges to $T(x)$ divided by the sum of the D_ms (for any x we like).

Weighted means of non-contiguous sets

If some of the C_ms can be zero, the relevant terms need not form a contiguous sequence; any finite collection of predecessors will do. To see what happens in these cases it is easier first to work with the sequence $V_n = D_{k-(n \bmod k)}U_n$. First, we divide the sequence V_n up into a sequence of row vectors $\mathbf{r}_x$, where

$$\mathbf{r}_x = [V_{kx-1} \quad V_{kx-2} \quad \ldots \quad V_{kx-k}].$$

Then we expand the terms in $\mathbf{r}_{x+1}$ into expressions of the terms in $\mathbf{r}_x$ using the recurrence relation on U_n elements. Using these expressions we can construct a matrix $\mathbf{P}$ such that $\mathbf{r}_{x+1} = \mathbf{r}_x\mathbf{P}$.

For example, when $k = 3$, $U_n = aU_{n-1} + bU_{n-2} + cU_{n-3}$, $D_1 = 1$ (we always get this), $D_2 = b + c$ and $D_3 = c$ (we always get $D_k = C_k$). So the first two row vectors are:

$$\begin{aligned} \mathbf{r}_1 &= [U_2 \quad (b+c)U_1 \quad cU_0], \\ \mathbf{r}_2 &= [U_5 \quad (b+c)U_4 \quad cU_3]. \end{aligned}$$

Expanding the terms in $\mathbf{r}_2$ using the recurrence relation (shown here as a column vector for readability) we get

$$\begin{aligned} \mathbf{r}_2 &= \begin{bmatrix} aU_4 + bU_3 + cU_2 \\ (b+c)(aU_3 + bU_2 + cU_1) \\ c(aU_2 + bU_1 + cU_0) \end{bmatrix} \\ &= \begin{bmatrix} (a^2+b)U_3 + (ab+c)U_2 + acU_1 \\ (b+c)((a^2+b)U_2 + (ab+c)U_1 + acU_0) \\ acU_2 + bcU_1 + c^2U_0 \end{bmatrix} \\ &= \begin{bmatrix} (a^3+2ab+c)U_2 + (b(a^2+b)+ac)U_1 + c(a^2+b)U_0 \\ (b+c)((a^2+b)U_2 + (ab+c)U_1 + acU_0) \\ acU_2 + bcU_1 + c^2U_0 \end{bmatrix}, \end{aligned}$$

so

$$\mathbf{P} \;=\; \begin{bmatrix} a^3+2ab+c & (b+c)(a^2+b) & ac \\ \dfrac{b(a^2+b)+ac}{b+c} & ab+c & \dfrac{bc}{b+c} \\ a^2+b & (b+c)a & c \end{bmatrix}.$$

(Note that $b+c>0$ since if c is zero then k is 2 rather than 3.) But

$$\sum_{c=1}^{3} P_{1,c} \;=\; a^3+2ab+c+(b+c)(a^2+b)+ac \;=\; 1,$$

$$\sum_{c=1}^{3} P_{2,c} \;=\; \frac{b(a^2+b)+ac+(b+c)(ab+c)+bc}{b+c} \;=\; 1$$

and

$$\sum_{c=1}^{3} P_{3,c} \;=\; a^2+b+(b+c)a+c \;=\; 1$$

(recalling that $a+b+c=1$). This means that $\mathbf{P}$ is row stochastic, i.e. it is square, all the elements are non-negative and each row sums to one. In fact this is the case for any value of k. We can see this by looking at the effect of expanding the largest U_n term on the sum of coefficients of other U_n terms. Since D_1 is always 1, the sum of the new coefficients of the U_{n-m} term will be $C_m + D_{m+1}$; but this is just D_m. So although the contributing values shift from column to column of the row vector the sum is preserved by the expansion. For the next expansion we now take advantage of the fact that the sum of the coefficients of U_{n-1} will have increased from D_2 to D_1 so the same method works until we have eliminated all unwanted U_n terms.

Once we have the stochastic matrix $\mathbf{P}$ we can determine the behaviour of $\mathbf{P}^n$ in the limit as $n \to \infty$ using some of the techniques for analysing transition matrices of Markov chains. The chain associated with the matrix is a directed graph with a vertex for each row and an edge for each non-zero matrix element $P_{r,c}$ from vertex r to vertex c labelled with the value of the matrix element. The edge labels are usually interpreted as probabilities of transitions between states, but in this case they represent changes in proportionate contributions to the value t; we also need to cope with the possibility of negative values in the row vector.

We need to define a few important features of these chains. A *communicating class* of vertices is a maximal class of vertices such that there is a path from every vertex in the class to every other vertex in the class.

It is *closed* if there are no edges directed to any vertices outside the class, otherwise it is *transient*. It is *periodic* if for any vertex, r, in the class the hcf of all lengths of paths from r to r is greater than one, in which case the period is the hcf of these path lengths.

Suppose column q corresponds to a vertex in a transient communicating class. Then there will be some $p < k$ such that column p is not in the transient class and the expansion of U_{kn+q+p} has a non-zero coefficient for U_{kn+q}; i.e. the expansion of U_n contains a U_{n-p} term. If q is the highest common factor of p and k then for large enough n there will be some power of p equal to any non-negative multiple of q modulo k. So all the columns whose indices are a multiple of q communicate; hence they must be members of the same transient class. This means that the expansion of U_{kn+q} has a non-zero coefficient for $U_{k(n-1)+q+p}$; i.e. column p will be in the transient class, a contradiction. So there will be no transient communicating classes in the chain for a recurrence relation.

If there is a periodic, closed communicating class for $\mathbf{P}$ then none of its vertices can communicate with themselves (as this gives a path of length 1 from the vertex to itself). But C_k cannot be zero so the expansion of U_n always has a non-zero coefficient for U_{n-k} which corresponds to the same vertex; i.e. in chains for recurrence relations all vertices communicate with themselves, so there are no periodic, closed communicating classes.

If we look at an aperiodic closed communicating class then we are interested in non-zero row vectors $\mathbf{u}$ such that $\mathbf{u} = \mathbf{uP'}$, where $\mathbf{P'}$ is the submatrix of $\mathbf{P}$ containing the rows and columns corresponding to the vertices of the closed class. These vectors correspond to stable solutions (either a single limit value or a repetitive cycle of values for V_n). Since the class is closed, $\mathbf{P'}$ is itself stochastic.

In an aperiodic class, for each column there is a finite integer such that there is a path from the vertex for that column to itself of any length greater than that integer. Even if the return paths all have length greater than one, their highest common factor is one. In the worst case we would have only two such lengths (in any case we can choose an arbitrary two), say p and q, then we can use these to construct paths of any length greater than $(p-1)(q-1)$. If we add to this the maximum of the shortest distances to all the other vertices then every other vertex can be reached from this one by a path of any length greater than this. Finally, take the maximum of all of these integers and raise $\mathbf{P'}$ to this power. The resulting matrix will not have any zero cells, and the corresponding chain will be the complete digraph of k vertices.

If we have a row vector $\mathbf{u}$ which contains both positive and negative column values, we can express it as $\mathbf{u}^- + \mathbf{u}^+$, where $\mathbf{u}^-$ is obtained from $\mathbf{u}$ by replacing any non-negative valued column by $-1/2$ and $\mathbf{u}^+$ by changing the non-positive values to $1/2$:

$$\mathbf{u}\mathbf{P}'^n \;=\; (\mathbf{u}^- + \mathbf{u}^+)\mathbf{P}'^n \;=\; \mathbf{u}^-\mathbf{P}'^n + \mathbf{u}^+\mathbf{P}'^n.$$

If a is the sum of the absolute values of columns in $\mathbf{u}^-$ then let $\mathbf{v}^-$ be the row vector obtained by dividing each column of $\mathbf{u}^-$ by $-a$:

$$\mathbf{u}^-\mathbf{P}'^n \;=\; (-a\mathbf{v}^-)\mathbf{P}'^n \;=\; -\,a(\mathbf{v}^-\mathbf{P}'^n).$$

Similarly, if b is the sum of the values in the positive valued row, then

$$\mathbf{u}^+\mathbf{P}'^n \;=\; (b\mathbf{v}^+)\mathbf{P}'^n \;=\; b(\mathbf{v}^+\mathbf{P}'^n).$$

Both $\mathbf{v}$ vectors lie within the $(k-1)$-dimensional simplex with vertices at each of the k standard basis vectors (e.g. a triangle for $k = 3$). The geometric effect of a stochastic matrix is a continuous map of this simplex into itself, and since $\mathbf{P}'^n$ is stochastic and has no zero cells it has no cells with value one, either, so the simplex is mapped strictly into its own interior.

The simplex is a compact convex set so by Brouwers Fixed Point Theorem there is at least one point which is fixed by the transformation. The length of lines in the image is strictly reduced by each application of the transformation. Each step divides the length by an amount greater than one, giving a decreasing sequence bounded below by zero and always less than the decreasing geometric sequence $(e/\sqrt{2})^n$, where e is the length of the longest edge of the image of the simplex, which tends to zero. This means there can only be one fixed point, and both $\mathbf{v}^-$ and $\mathbf{v}^+$ will tend to this point, so $\mathbf{u}$ must tend to $(b-a)\mathbf{v}$ where $\mathbf{v}$ is the fixed point. The value $b-a$ is just the sum of the column values of $\mathbf{u}$, which is that portion of t which is contained in the class.

The result we have is that all recurrence relations of the form

$$U_n \;=\; \sum_{m=1}^{k} C_m U_{n-m},$$

where

$$\sum_{m=1}^{k} C_m \;=\; 1, \qquad 1 > C_1,\; C_2,\; \ldots,\; C_{k-1} \geq 0,\; C_k > 0,$$

converge to a repeating pattern of length k whose precise values we can determine analytically by solving just the set of simultaneous linear equations embodied in the eigenvector equation

$$\mathbf{P} - \mathbf{I} = \mathbf{0}$$

and using the Markov chain for $\mathbf{P}$ to identify the closed communicating classes. The proportion of t allocated to each closed class will be the same as that in the initial sequence and it will be distributed across the terms in the V_n sequence in the class in proportions given by the eigenvector. The U_n sequence can be derived from the V_ns simply by dividing by the appropriate $D_{k-n \bmod k}$ values. Notably, we do not need to solve an auxiliary equation to find an eigenvalue (which is useful when k is large) and all the procedures involved are mechanical.

Problem 182.1 – Reverse and square

Eddie Kent

This is really exciting, looking through old newspapers. Apparently someone asked for a number which, when reversed and squared, will give its own squared value in reverse.

The answer given was 13. But the Bishop of Peterborough wrote in to point out that the same is clearly true of 10, but also of 11 and 12 (11 is a palindrome whose square is also palindromic).

He then went on to say that the construction is true of many more numbers (indeed, infinitely many, since they include $a10^n + b$, $n = 2, 3, \ldots$, for $1 \le a, b \le 3$).

This suggests a problem: Find all solutions of

$$\begin{aligned}(10^m a_m + 10^{m-1}a_{m-1} + \cdots + 10a_1 + a_0)^2 \\ = 10^n b_n + 10^{n-1}b_{n-1} + \cdots + 10b_1 + b_0, \\ (10^m a_0 + 10^{m-1}a_1 + \cdots + 10a_{m-1} + a_m)^2 \\ = 10^n b_0 + 10^{n-1}b_1 + \cdots + 10b_{n-1} + b_n\end{aligned}$$

in non-negative integers m, n, a_0, a_1, …, a_m, b_0, b_1, …, b_n subject to the familiar conditions that govern the representation of integers in the decimal system: $0 \le a_1, a_2, \ldots, a_{m-1}, b_1, b_2, \ldots, b_{n-1} \le 9$ and $1 \le a_0, a_m, b_0, b_n \le 9$.

1,000,000,000. (Abelian groups are commutative.)

Solution 180.7 – Interesting series

Find the sum of this infinite series:

$$S(x) = \frac{1}{1+x} + \frac{x}{(1+x)(1+x^2)} + \cdots + \frac{x^{2^n-1}}{(1+x)(1+x^2)\ldots(1+x^{2^n})} + \ldots.$$

John Bull

The series is clearly undefined for $x = -1$. For $x = 1$ the series is a simple geometric progression and it is easily shown that $S(1) = 1$.

Multiply by $1/(1-x)$ and repeatedly use the identity $(1-a)(1+a) = 1-a^2$. Then

$$\frac{S(x)}{1-x} = \frac{1}{1-x^2} + \frac{x}{1-x^4} + \frac{x^3}{1-x^8} + \cdots + \frac{x^{2^{n-1}-1}}{1-x^{2^n}} + \ldots.$$

Split each term into partial fractions

$$\begin{aligned}\frac{S(x)}{1-x} &= \left(\frac{1}{1-x} - \frac{x}{1-x^2}\right) + \left(\frac{x}{1-x^2} - \frac{x^3}{1-x^4}\right) \\ &\quad + \left(\frac{x^3}{1-x^4} - \frac{x^7}{1-x^8}\right) + \cdots + \left(\frac{x^{2^{n-1}-1}}{1-x^{2^{n-1}}} - \frac{x^{2^n-1}}{1-x^{2^n}}\right) + \ldots \\ &= \frac{1}{1-x} - \frac{x^{2^n-1}}{1-x^{2^n}} + \ldots.\end{aligned}$$

Now multiply by $1-x$ and let $n \to \infty$. Then

$$S(x) = 1 - \frac{(1-x)x^{2^n-1}}{1-x^{2^n}} + \ldots \to \begin{cases} 1 & \text{if } |x| < 1 \\ 1 + \dfrac{1-x}{x} = \dfrac{1}{x} & \text{if } |x| > 1. \end{cases}$$

Problem 182.2 – Nine tarts

Dick Boardman

There are nine jam tarts. Some jam has been removed from one and put back into another so that seven weigh the same, one weighs a bit more and one a bit less. Find the light and heavy tarts in the minimum number of weighings.

(By a *weighing* we mean the process of selecting two sets of tarts, A, B, and determining whether A is lighter than B, A is heavier than B, or A has the same weight as B.)

Authentication and key exchange

John Bull

This article complements the one I published in M500 **176** – 'Keyless and deniable encryption.' By way of introduction I tell a well-known story concerning the Russian postal system.

In Cold War days the Russian post office was notoriously corrupt. Any parcels that could easily be opened were opened in the sorting office and the contents stolen. Any parcels that were difficult to open were allowed through. These tactics provided sufficient illegal profit for corrupt postal workers.

Boris in Moscow had bought a valuable gem for his girlfriend Natasha in Gorki and wanted to send it to her. They agreed a strategy by telephone. What was it?

Boris put the gem in a box and attached a padlock. The box was difficult to open so the post office allowed it through. But Natasha couldn't open it either because she didn't have a key. So she added a padlock of her own and sent the box, now secured with two padlocks, back to Boris. Boris removed his own padlock and sent the box, still secured with her padlock, back to Natasha. Natasha removed her padlock and retrieved the gem.

This simple idea underpins the keyless encryption strategy that I described in M500 **176**. It might provide a flash of insight having first been presented with the number theory formulation.

But there is a problem. Suppose Ivan, an intelligent corrupt postal worker, reasons that Boris and Natasha are following this strategy. Ivan attaches his own padlock and sends the box back to Boris without ever passing it on to Natasha. Boris, assuming that the box had been returned from Natasha, removes his padlock and sends it back. Ivan intercepts it, removes his padlock, and retrieves the gem. Ivan simply masquerades as Natasha. What countermeasures could Boris and Natasha deploy against this attack?

It is not easy to see a simple solution based on boxes and padlocks. The approach suggested here is an exchange of letters first to agree the specification of a padlock and key and then use this padlock to secure the box in transit.

Boris and Natasha have to devise a method that will allow each to know that any letters they exchange have come from the other and be confident that anyone reading them in transit cannot make use of them. They can only do this by way of a secret they share; a codeword 'BoLovesNat' they agreed when they last spent the night together in Minsk.

The protocol that follows requires an encryption algorithm. One based

on the one-way properties of the discrete logarithm was introduced in the previous article in M500 **176** and it is recalled in the annex at the end of this article. In what follows the notation $\{m\}k$ denotes a requirement for encryption of a message m using key k.

The problem with using 'BoLovesNat' directly as a key is that an attacker might guess it, and even if buried in a one-way function he could try many guesses until one fits. A way round this is to ensure that a key derived from 'BoLovesNat' is only ever used to encrypt random quantities, thus making it impossible for an attacker to know if his guess had succeeded.

Boris derives a key p from the codeword $p = g^w \bmod n$ (where $w =$ 'BoLoves Nat') and initiates the following exchange:

1. Boris to Natasha: $\{g^x,\ i\}p$
2. Natasha to Boris: $\{g^y,\ j\}p$, $\{i\}g^{xy}$
3. Boris to Natasha: $\{j\}g^{yx}$

Here, i, j, x and y are all cryptographic quality random numbers and all numbers are modulo n.

Boris chooses i and x, creates g^x, concatenates g^x with i, encrypts $(g^x,\ i)$ with p, and sends this to Natasha. Natasha can create p, so she decrypts to recover g^x and i.

At this stage Natasha cannot be satisfied that the message came from Boris. Had Ivan intercepted and substituted an equivalent sized bundle of bits Natasha would have recovered something but not the g^x and i Boris intended. By step 3 Natasha will be satisfied.

Ivan cannot do anything with $\{g^x,\ i\}p$ because it would be impossible to know if a guess of w which recovered the real g^x and i were actually correct. Both g^x and i are random quantities and include no testable information.

Natasha chooses j and y and forms $s = (g^x)^y \bmod n = g^xy \bmod n$ [8]. This is the key that opens the padlock. Natasha chooses j and y, concatenates g^y with j, encrypts $(g^y,\ j)$ with p, and sends this to Boris. She also sends i encrypted with the key s; that is, she sends $\{i\}g^{xy}$.

Boris decrypts $\{g^y, j\}p$ to recover g^y and j and forms $s = (g^y)^x \bmod n = g^{yx} \bmod n$. Because $s \equiv g^xy \equiv g^yx \pmod n$, both Boris and Natasha now hold the same key, s. Boris uses this to recover i and if the quantity he recovers is the same as the i he sent he knows that both components of the message in step 2 must have come from Natasha. Other than by a guess, no-one apart from Boris and Natasha could create p.

Boris sends j encrypted with the key s back to Natasha; that is, he sends $\{j\}g^{yx}$. Natasha decrypts this to recover j and if the quantity she recovers is the same as the j she sent, she knows that the messages in steps 1 and 3 must both have come from Boris.

Both Boris and Natasha now hold the specification of the same padlock key s and can use this to send the gem. Alternatively, other information encrypted under s could be sent in parts 2 and 3 of the protocol (but not encrypted under p without weakening the protocol). In effect this is keyless encryption. Otherwise s may be retained and reused as an encryption key. This protocol enables transmission of secret information while also being secure against masquerade and man-in-the-middle attacks.

It is possible that Ivan vandalises the protocol without stealing anything, or simply fails to pass on messages, known as denial of service attacks, but it is impossible to deal with these. At least, in theory, Boris and Natasha know that no-one else will purloin their token of love!

Another type of attack on protocols of this nature is for Ivan to collect all the bits from all the messages and try to use them together to derive the encrypted quantities. This is rather like trying to solve a very complex set of simultaneous equations. This is impossible in this case because there are no simultaneous variables, which is not true of similar protocols. Also no other known protocols work in as few as three exchanges. For alternatives see [2–6].

A protocol very closely related to the one in this article is the subject of a pending patent application in the USA (with myself as co-inventor). This is the first publication but the description is substantially condensed and simplified for presentation in M500.

References

[1] John Bull and Dave Otway, 'A nested mutual authentication protocol', *Operating Systems Review*, vol. 33, no. 4 (Oct 1999), 42–47.

[2] Thomas Wu, Department of Computer Science, Stanford University, 'The secure remote password protocol', 1998 *Internet Society Symposium on Network and Distributed System Security.*

[3] Mark Lomas, Li Gong, Jerome Saltzer and Roger Needham, 'Reducing risks from poorly chosen keys', 1989 *ACM* 089791-338-3/89/0012/0014.

[4] Martin Abadi, Mark Lomas and Roger Needham, 'Strengthening passwords', *Digital Systems Research Centre Technical Note* 1997-033, http://www. research.digital.com/SRC/, 4 Sep 1997, revised 16 Dec 1997.

[5] Steven Bellovin and Michael Merritt, 'Augmented encrypted key exchange: a password-based protocol secure against dictionary attacks and password file compromise'. This can be found at various web sites. The original 'unaugmented' version was *Proceedings of the IEEE Symposium on Research in Security and Privacy*, Oakland 1992.

[6] David P. Jablon, 'Strong password-only authenticated key exchange', *ACM Computer Communications Review*, vol. 26, no. 5 (Oct 1996). A

later revision was distributed by the author in private correspondence.

[7] L.Blum, K.Blum and M.Shub, 'A simple unpredictable random number generator', *SIAM Journal on Computing*, vol. 15 (1986), 364–383.

[8] Whitfield Diffie and Martin Hellman, 'New directions in cryptography', *Transactions on Information Theory*, vol. IT–22, no. 6 (Nov 1976), 644–654.

[9] 'National Institute for Standards and Technology, NIST FIPS PUB 186', *Digital Signature Standard*, US Department of Commerce, May 1994.

Annex – Discrete Logarithm Encryption

Denote encryption of a message m using key k as $\{m\}k$; then the encrypted cyphertext is given by $\{m\}k = m \oplus g^{r \oplus k} \bmod n$, where

- n is usually, but not necessarily, chosen to be a large prime;
- the generator g is a primitive root of n;
- the number r is a cryptographic quality random number, which implies that if generated by a psuedo random number generator there is no discernible correspondence between r and any other future or past number in the pseudo random sequence [7];
- all of the numbers k, n and r are typically large, say of order 1024 bits;
- g is typically small, say of order 4 bits.

There has been much debate about choosing values for g and n for standardization and additional constraints are applied; for example, n is chosen such that both n and $(n-1)/2$ are prime [9]. A full discussion is beyond the scope of this article. Note that the above implies that $g^{r \oplus k} \bmod n$ will also be of order 1024 bits; the operator $\oplus$ denotes a bitwise exclusive-or operation.

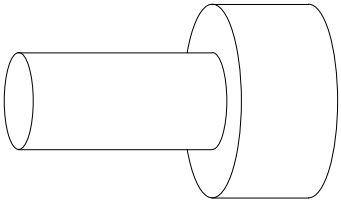
The message m is of the same order of size as n, say 1024 bits. In a practical implementation, a long message m would be broken up and/or padded into blocks of 1024 bits, the blocks transmitted separately, and the decrypted output of each block reassembled into the message. In practice, earlier components would also be chained or fused into later components, but again this is beyond the scope of this article.

The random number r is concatenated with $\{m\}k$ for transmission; that is, $(r, \{m\}k)$ is sent. The recipient will need to recover r, use it to recreate $g^{r \oplus k} \bmod n$, and use this to recover the message by $m = (\{m\}k) \oplus g^{r \oplus k} \bmod n$. Alternatively a commercial encryption package could be used but the protocol in this article would not then be self contained.

Solution 179.4 – Two cylinders

Dick Boardman

Two cylinders have radii R, r and lengths L, l, respectively, with $R > r > 0$ and $l > L > 0$. They are placed next to each other with their axes co-linear. How long is the shortest loop of string that can be passed over the fat cylinder onto the thin cylinder?



If the fat cylinder is greater than a certain length, the answer is simply its circumference. If the thin cylinder is missing, the shortest length is $2L+4R$ and this is also a lower bound for this problem.

However, for short cylinders a second solution is possible. (Note that the length of the thin cylinder is not used.) Imagine a slippery elastic band, initially dangling loosely around the thin cylinder. Imagine it stretched, round the thin cylinder, across the face of the fat cylinder, then across its circumference until it reaches the far edge of the fat cylinder and finally across the far face of the fat cylinder. The two sides will be symmetrical and will each comprise four sections.

(i) A circular section around the thin cylinder, against the face of the fat cylinder. The length of this section will be $r\theta$, where θ is the angle from the vertical to the point where the band leaves the thin cylinder.

(ii) A straight section across the face of the fat cylinder to its edge at a point P with co-ordinates (P_x, P_y). The length of this section is fixed. It is $\sqrt{R^2 - r^2}$. Also the value of P_y may be positive or negative, ranging from r to $-R$. Let $\phi = \arctan(P_y/P_x) = \arcsin(P_y/R)$. Then $\theta = \arcsin(r/R) - \phi$.

(iii) A curved section around the circumference of the fat cylinder meeting the far face at Q. Let the coordinates of Q be (Q_x, Q_y) and note that Q_y may be positive or negative.

(iv) A straight line across the far face of length $\sqrt{R^2 - Q_y^2}$.

Assume that the band is very thin. Then the length of the curved section can best be seen by imagining the circumference of the fat cylinder unrolled until it forms a plane. This will be a rectangle with sides L and $|Q_y - P_y|$. The shortest path across will be a straight line of length $\sqrt{(Q_y - P_y)^2 + L^2}$.

For any specific pair of cylinders, the total length of the path will be a function of P_y and Q_y since ϕ and θ can be calculated from P_y and Q_y. In order that the loop may pass over the cylinders it must have length at least

the maximum with respect to Q_y. However, for any particular value of Q_y we may minimize with respect toP_y.

To find the minimum, differentiate the total path length with respect to P_y and equate to zero. Solving this gives the best value for P_y for a given Q_y. If we plot these best values against Q_y we get a curve with a maximum, and this is the shortest loop length that will pass right over. The 3-dimensional graph of path length against P_y and Q_y will be saddle shaped close to this point and the required value will be the flat point of the saddle.

To find this point, differentiate the total path length with respect to P_y and Q_y and equate both expressions to zero. These simultaneous equations may be solved numerically for P_y and Q_y and from this the minimum length that will just pass over the cylinders found.

As an example, let $r = 1$, $R = 5$, $L = 2$. Using MATHEMATICA, this case has a minimum at $Q_y = -0.986893$ and $P_y = -0.575795$, and the minimum length of the string loop is 24.3184.

Solution 177.4 – e in nine digits

> Find the best approximation of the mathematical constant e = 2.7182818... using only the digits 1 through 9 inclusive—once and only once each. Addition, division, multiplication, subtraction, exponentiation, parentheses and decimal points—and nothing else—are allowed.

ADF

Nobody sent anything, so I thought I would have a go. Recall that for large n the quantity $(1+1/n)^n$ differs from e by approximately $e/(2n)$. This was proved in an article by John Reade published in M500 **29** and reprinted in M500 **178**, page 41, especially for the benefit of would be solvers of this problem.

Split the digits $\{2, 3, \ldots, 9\}$ between n and $1/n$. Here's one way:

$$n \;=\; 5^{9^{6+8}} \;=\; 5^{22876792454961}, \quad \frac{1}{n} \;=\; (.2)^{3^{4\cdot 7}} \;=\; 5^{-22876792454961}.$$

Thus

$$e - \left(1 + (.2)^{3^{4\cdot 7}}\right)^{5^{9^{6+8}}} \;\approx\; \frac{e}{2} \cdot 5^{-3^{28}} \;\approx\; 10^{-15990191721438}.$$

Solution 180.3 – Fence

A farmer has an L-shaped barn which measures $80' \times 80'$ with a $30' \times 40'$ rectangle cut out of one corner. He also has a $50'$ roll of fencing which he wants to use to enclose a grazing area next to the barn. What is his largest possible grazing area?

Tony Forbes

Interesting problem. The awkwardness arises from $30 < 100/\pi$. If the short wall of the L-shaped part were a little less short, a quarter circle would enclose an area of about 795.7747.

Ralph Hancock suggests a quarter ellipse with semi-axes 30 and w, say. Using the arc-length formula for the ellipse $(x/w)^2 + (y/30)^2 = 1$, we obtain this expression for the length of the fence:

$$\int_0^w \sqrt{1 + \frac{900x^2}{w^2(w^2 - x^2)}}\, dx \;=\; w \int_0^{\pi/2} \sqrt{1 - m \sin^2\theta}\, d\theta,$$

where $m = 1 - 900/w^2$. Experts will probably recognize the last integral as $E(m)$, the *complete elliptic integral of the second kind.* The rest is straightforward. Solve $wE(m) = 50$ for w and compute the area of the elliptical quadrant as $30w\pi/4$. The result is $w \approx 33.6107$, area ≈ 791.9341.

Ron Potkin (who submitted the problem) sent this solution: The grazing area comprises a circular quadrant of radius 30 connected to a $(50 - 15\pi) \times 30$ rectangle. The short side of the grazing area is 30 and the long side approximately 32.8761. Its area is $1500 - 225\pi \approx 793.1417$. It is possible to do slightly better with a continuous circular arc. There is a formula for this one floating around out there somewhere. I was hoping one of you may have seen it.

Well, let's try it. Consider an arc of a circle with radius r and centre (x, y) relative to the corner where the walls of the L-shaped part meet. Assume that one end of the fence is fixed to the far end of the $30'$ wall and the other end is somewhere on the $40'$ wall. If $|x|$ and $|y|$ are not too large (a diagram helps here),

$$y \;=\; 30 - \sqrt{r^2 - x^2}, \tag{1}$$

$$\frac{50}{r} \;=\; \frac{\pi}{2} + \arcsin\frac{x}{r} + \arcsin\frac{y}{r} \tag{2}$$

and the area is

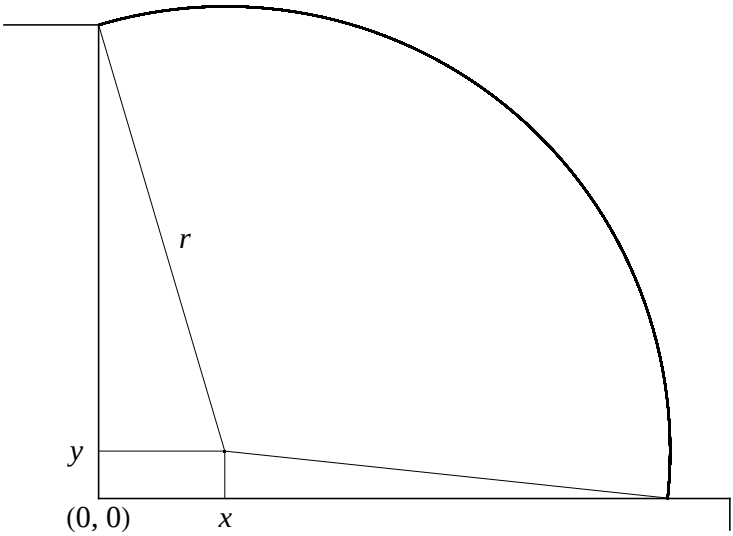
$$A(r) \;=\; 25r + xy + \frac{x}{2}\sqrt{r^2 - x^2} + \frac{y}{2}\sqrt{r^2 - y^2}. \qquad (3)$$

Now I have to admit that I actually solved (1) and (2) to obtain a formula for x in terms of r. I substituted the resulting expression for x in (3) and differentiated. That would have been a good point to give up. When dA/dr is evaluated as a function of r it is truly horrendous, and when I solved $dA/dr = 0$ numerically I found (amongst other things) that $y \approx 0$. Then the penny dropped!

Look at the diagram. If $y > 0$, the circular fence curves inwards to meet the $40'$ wall and the grazing area is obviously not maximal.

So let us assume $y = 0$. The area is now $25r + 15x$, where $x = -r\cos(50/r)$ and $x^2 + 30^2 = r^2$. Hence $(1 - \cos^2(50/r))r^2 = 30$ and numerical methods give the approximate solution

$$r \;=\; 30.11985026, \quad x \;=\; 2.684283818, \quad A(r) \;=\; 793.26051374.$$



The one thing we can be certain of is that there is no intelligent life anywhere in the Solar System, except possibly on Earth.—Patrick Moore.

Kiwi fruit

Eddie Kent

I sent this letter to a London outfitter.

> Dear Sirs,
> The last time I was in the City I called in for some new trousers, having splashed a pair with creosote which won't seem to come out. You had the trousers at £25 a pair or £39 for two. I think that was it. I said I would have two. The boy hunted but could only find one. I said, OK I'll give you £20 for one. He refused.
>
> My argument was, if there was only one left and they come in as pairs (as they must, otherwise you can't guarantee that offer) then someone must have bought one pair, at £25. Therefore with my £20 for the other you would have £45 for two instead of £39—an extra £6. I on the other hand would only be £5 better off. Free money all round with you taking the larger portion. What could be wrong with that?
>
> However, no deal, so no trousers. It seems to me a funny way to do business, but it is your shop so you must be left to run it to suit yourselves. But as a point of interest, supposing I went to a branch that actually had stock, where this offer was on, and asked for three pairs. How much would that cost?
>
> Yours, etc.

ADF writes—Kingston upon Thames market traders are familiar with this kind of reasoning. They often advertise things at x pence, N for y pence, where $y < Nx$, and will always let you buy M items for $[yM/N]$ pence if $M \geq N$. On the other hand, most 'proper' shops charge $[M/N]y + (M - N[M/N])x$ pence because their well-educated staff are better adapted to computing that relatively complicated expression. (We're using the standard notation $[z]$ for the largest integer $\leq z$.) Eddie also sent me this.

> A man and a woman were clinging on to a rope over a deep ravine with certain death below them. *The rope started fraying.* They agreed that it could only support one of them till the rescuers arrived. Who would let go? Finally the woman gave a really touching speech saying how she would give up her life to save the man, because women were used to giving up things for their husbands and children and giving in to men. 'Bravo!', said the man. And clapped.

Most amusing, I thought, remembering that 'James Bond' film sequence which has the man trying to board an already airborne aircraft by climbing up a rope dangling from the cargo hold. The rope starts fraying. Strands break. Excitement mounts.

Alas! It is not possible! In each case the rope breaks catastrophically. If N strands cannot support a load, $N-1$ strands are even less capable of supporting the same load. This is because $N-1 < N$.

The grocery retail business, on the other hand, provides some interesting counter-examples. My local supermarket regularly has those curious special offers the like of which I wrote about in **176**. Typically,

Lasagne: 99p each, buy two and save £1.

If you require only one packet of lasagne, remember to buy it twice.

However, strangest of all was an experience involving minced beef. The offer was

Mince, £1.79; buy one, get one free; reduced to 89p.

It happened that the 'get one free' part applied to the full price, so two items came to −1p after deducting £1.79 from two 89ps.

Solution 180.2 – Unlimited prize

A six-sided die is thrown repeatedly. When all the numbers 1, 2, ..., 6 have appeared, then B pays A £(number of throws). What must A pay B to make the game fair?

Michael Adamson

The question is essentially analogous to 'How many cereal packets need to be bought on average to complete a collection of six different plastic animals if each box contains one animal out of the six at random?'

After five different numbers have been obtained, the likelihood that the next roll will produce the sixth number is 1/6; so on average 6 rolls are required.

Working backwards, a similar argument shows that 3 rolls are required to obtain the fifth number (which can be either of two remaining), 2 for the fourth, 3/2 for the third, 6/5 for the second, and 1 for the first (the first roll always produces a wanted number).

In total, therefore, $14\frac{7}{10}$ is the expected number required, and this is the correct stake for a fair game.

Problem 182.3 – Russian roulette

John Bull

Is there any way to modify the rules of Russian roulette to make it fair for both players; that is, so that in any long run game each player has an equal chance of losing? Possibilities that come to mind are: vary the number of bullets in a defined way for a given turn; define some turns on which the chamber is not spun; define a variation to the sequencing, such as: A, B, B, A, A, B, B, B, etc. If it is not possible to achieve absolute equality, what is the fairest strategy that can be devised? Can it be proven that there is never any way to compensate for the disadvantage of a person having to go first?

[*Russian roulette* is a game for two players. It involves a six-chamber revolver loaded with one bullet. Under the usual rules players take turns to spin the chamber assembly and fire the gun. The player who discharges the bullet loses.]

Meat and three veg

Eddie Kent

It is not every day that one sees a mathematical equation in a newspaper, though Benny Green used to say that *The Times* was the only paper that could set one. This, however, was not in *The Times* and hence (or otherwise) took a bit of sorting out. This is how it looked: %Gravy uptake = W – (D/S) Divided by D, X 100.

After a couple of trials I got it to look like this: $G = \frac{W-D/S}{D}$, where G is percentage of gravy uptake, W is uncooked or 'wet' weight of food, D is cooked, or 'dry' weight and S is the shrinkage factor.

The equation was devised by a Dr Fisher, who is employed by Bisto, and is intended to show that you cannot have too much gravy on your roast dinner. You just have to be careful over the order in which you eat the various foods on your plate. For instance, Yorkshire pudding has the highest absorbency rate and can be shown to have 'a 90 per cent gravy uptake: $W = 47.5$ grams; $D = 25$ grams; shrinkage factor is zero.' (*Sic*).

I imagine that if the pudding doesn't shrink we can give the value 1 (not 0) to S. Then simple substitution gives the stated value.

From Dr Fisher's research it is clear that you should eat the meat first as this absorbs the least gravy, followed by green vegetables at 15 per cent in 30 seconds and roast potatoes at 30 per cent. This actually contradicts my memory as a boy when we had roast every Sunday. I'm sure I found I could mop up any amount of gravy with potatoes, at any time I chose; and my mother never used Bisto.

Problem 182.4 – Four coins

Four coins are arranged in a circle. You cannot see them. You choose one or more numbers between 1 and 4. Your opponent inverts the coins in the positions which you selected. The positions are numbered 1, 2, 3, 4 clockwise around the circle but your opponent is free to choose which coin is in position 1.

If the result is four heads, the game stops and you win. Otherwise the procedure is repeated.

Devise a winning strategy.

Problem 182.5 – Two £10 notes

John Bull

A first ten pound note is laid flat on a table. A second ten pound note is crumpled and placed on top of the first so that none of it protrudes beyond the edges of the first.

Prove that there is at least one point of the second note that is directly above a corresponding point of the first. [Hint: see p. 7.]

Problem 182.6 – n balls

John Bull

There are n balls in an urn, all of different colours. Two balls are removed at random. The second of the pair is painted to match the first and the two balls replaced. The balls are thoroughly mixed and again two balls are removed at random. Again the second of the pair is painted to match the first and the balls replaced. This process is continued.

What is the expected number of turns required before all the balls are the same colour?

Problem 182.7 – Three cos and three sins

John Bull

Let a, b, c be real numbers that satisfy both $\cos a + \cos b + \cos c = 0$ and $\sin a + \sin b + \sin c = 0$. Show that

$$\cos 2a + \cos 2b + \cos 2c \;=\; \sin 2a + \sin 2b + \sin 2c \;=\; 0.$$

Hamming

Jeremy Humphries

Here's something strange. I think. I was browsing in the area of Programme Delivery Control (PDC) numbers. These are the numbers they print in the Radio Times so that you can preset your video recorder. I was searching for somewhere on the web that publishes them.

I didn't find anywhere which would tell me the values for today's TV broadcasts, but I did find no end of stuff dealing with the technical side of the matter. Among the technical stuff, I found much on Hamming codes. I give a bit of extract below.

The writer of this piece seems to treat 'hamming' as the present participle of the verb 'to hamm', so that a hamming code is a code which hamms data. He refers to bytes which result from the transformation as hammed bytes. I also found the expression 'to de-hamm' used for the reverse of the process.

Now everybody who has done any coding theory knows that Hamming codes are named for Richard Wesley Hamming (1915–1998), who invented the idea. Is it the case that he has actually become a verb in accepted usage, or does the bloke writing below just not realize where the word comes from?

I remember once, when I was studying the OU Gödel course, a fellow engineer at work saw me reading a book on Turing machines in the dinner break. He came over and asked me what these turing machines were like, and what was the meaning of 'to ture'. Honest. He was absolutely serious.

Also, somebody once asked me if there was a lightside layer, analogous to the Heaviside layer.

Several Teletext packets contain information protected by hamming. This is a method for encoding data such that errors in reception can be detected and, if the error is sufficiently small, corrected. Teletext uses two hamming codes.

The simpler and more robust version encodes 4 bits of data in one 8-bit byte. This code is used extensively to protect the fields that have meaning to the Teletext system itself. The more efficient code encodes 18 bits of data in three 8-bit bytes. It is used to protect some of the data fields inside Teletext packets. Both codes are designed such that any one-bit error can be corrected, and any 2-bit error can be detected.

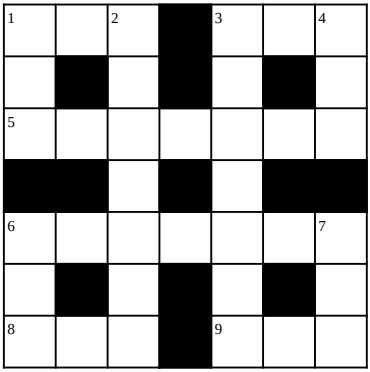
The 8/4 code is quite simple; if the input nibble is the 4-bit value: b_3, b_2, b_1, b_0 with b_3 being the most significant bit, then the output hammed byte is the 8-bit value: b_3, $b_3 \oplus b_2 \oplus b_1$, b_2, $\overline{b_2} \oplus b_1 \oplus b_0$, b_1, $\overline{b_3} \oplus b_1 \oplus b_0$, b_0, $\overline{b_3} \oplus b_2 \oplus b_0$, where $\oplus$ represents bitwise exclusive-or and the bar denotes bitwise not.

This code has the property that every value is four bits different from all other such values. A one-bit error is therefore unambiguously correctable, being only one bit away from a valid code. A two-bit error is detectable but not correctable, being equidistant between two valid codes. Here is the table of all 16 encoded nibbles.

$0 = 0000 \to 15 = 00010101$	$8\ 1000 \to D0 = 11010000$
$1 = 0001 \to 02 = 00000010$	$9\ 1001 \to C7 = 11000111$
$2 = 0010 \to 49 = 01001001$	$A\ 1010 \to 8C = 10001100$
$3 = 0011 \to 5E = 01011110$	$B\ 1011 \to 9B = 10011011$
$4 = 0100 \to 64 = 01100100$	$C\ 1100 \to A1 = 10100001$
$5 = 0101 \to 73 = 01110011$	$D\ 1101 \to B6 = 10110110$
$6 = 0110 \to 38 = 00111000$	$E\ 1110 \to FD = 11111101$
$7 = 0111 \to 2F = 00101111$	$F\ 1111 \to EA = 11101010$

Crossnumber

ADF



Across

1 $\sqrt[3]{3 \text{ dn.}}$

3 $\dfrac{5 \text{ ac.}}{(4 \text{ dn.})(1 \text{ ac.})}$

5 $(1 \text{ ac.})(3 \text{ ac.})(4 \text{ dn.})$

6 $((9 \text{ ac.}) - (3 \text{ ac.}))(1 \text{ ac.})(8 \text{ ac.})$

8 $\dfrac{6 \text{ ac.}}{((9 \text{ ac.}) - (3 \text{ ac.}))(1 \text{ ac.})}$

9 $\dfrac{6 \text{ ac.}}{(1 \text{ ac.})(8 \text{ ac.})} + (3 \text{ ac.})$

Down

1 $\sqrt[3]{2 \text{ dn.}}$

2 $(1 \text{ dn.})^3$

3 $(1 \text{ ac.})^3$

4 $\dfrac{5 \text{ ac.}}{(1 \text{ ac.})(3 \text{ ac.})}$

6 $3\,(1 \text{ dn.})$

7 $(3 \text{ ac.}) + (6 \text{ dn.})$

Scientist: Pascal, being French, created a vacuum at the top of a column of wine supported by atmospheric pressure.

Presenter: I expect he had the wine left over from his pasteurization experiments.—R4. [Spotted by JRH.]

Letters to the Editors

Two envelopes

Dear Editor,

Whether the following is a mathematical problem or a philosophical one I hesitate to surmise; the argument is superficially convincing whilst obviously flawed.

The game-show host offers the player two sealed envelopes one of which contains twice as much money as the other. The player chooses one, opens it and then decides whether to keep it or exchange it for the other envelope.

Given the information that one contains twice as much money as the other, the player having opened one of the envelopes and ascertained its contents, x, say, will always elect to choose the other as it has either x more or $x/2$ less. Can this be logical?

Michael Adamson

ADF—Is there a ratio which is not paradoxical?

Chimps

Dear Tony,

This is the best I can come up with in changing CHIMP to WOMAN, not an easy task!

CHIMP, CHIME, CHINE, SHINE, SHINS, SHIES, SHOES, SHOPS, CHOPS, COOPS, COMPS, COMAS, ROMAS, ROMAN, WOMAN.

ROMAS is a plural form of ROM, which is a Romany gypsy man. I expect there is a shorter route but I couldn't find one.

Christine White

Old age

Dear Jeremy,

I attach a copy of an exchange between people from a mailing list of genealogists trying to work out whether a method of calculating dates should work. I think I have seen something like it before. Going by the way he writes, I think Derek must be a mathematician. I know nothing definite about any of the people involved in this exchange.

Colin Davies

ADF writes—It's based on the magic number **8870**. This is the number you need if you want to find the birthdate of someone from his date of death and his age, assuming you have the latter in years, months and days.

An American historical/genealogical society gives a simple procedure which works something like this:

Suppose the person died on 19 June, 1800, at the age of 170 years, 8 months, 29 days.

1. Start with the year, month and day	18000619
2. Subtract the age at death	1700829
	16299790
3. Subtract 8870	8870
	16290920

Hence the person was born on 20 September 1629.

The result of step 3 should not be taken too literally. Often you will end up with a funny date which will require a minor adjustment or two. But the amazing thing is that the formula works. At least some of the time.

Derek Peasy points out some flaws. There is obviously no mechanism for dealing with leap years, let alone the change from the Julian to the Gregorian calendar. Derek says:

> Using an age of 67 years exactly on 24 Dec 2000, I have discovered it has some problems, though it gets quite close.
> 23 Dec 2000, age 661129, birthday: 19331224 ⇒ 24 Dec 1933
> 24 Nov 2000, age 661100, birthday:
> 19331154 ⇒ 54 Nov 1933 ⇒ 24 Dec 1933
> 24 Dec 2000, age 670000, birthday:
> 19322354 ⇒ 54 23 1932 ⇒ 54 Nov 1933 ⇒ 24 Dec 1933
> 01 Jan 2001, age 670008, birthday: 19931223 ⇒ 23 Dec 1933
> Were it correct it would be very elegant. Even with the small errors and notational problems that I have identified, it is interesting. I wonder what is the biggest error that it can produce?

My immediate observation is that the digits 8870 indicate a 12-month year and a constant 30-day month. Since $365/12 \approx 30.4$ it is possible that 8869.6 might work better. Older readers may remember this kind of thing from doing arithmetic in pounds, shillings and pence. The relevant digits are 8088 and it never fails.

It's true. A living 170-year-old really did exist. See, for example, 'Comparative View of the Duration of Life among Centenarians', Table IX, *Willich's Popular Tables*, 1852 edition; review: M500 **129**, p. 9.

Multiples of eleven

Dear Tony,

You probably know that any row of Pascal's triangle gives a power of eleven, and this is valid if we accept columns containing more than 9. In fact, as a number every row is equal to $(r+1)^n$ with r in an unspecified base. This depends on the remainder theorem, of course, from which the rule for divisibility by 11 is drawn. Recall that a number is divisible by 11 if and only if the $+/-$ alternating sum of its digits is also divisible by 11.

Now I ask myself, what is the condition that a sum of digits with $+/-$ alternating signs adds to a multiple of 11 other than zero. Believe it or not, I still don't have a maths program on my computer so I am reduced to using a pocket calculator. You will see a pattern emerging which for a few r gives the rule: $(19+9x)\cdot 11 \to 11$ for $x = 0, 1, 2, \ldots, 7$. Also, for example,

$$28\cdot 11 = 308 \ \to\ 11, \quad 29\cdot 11 = 319 \ \to\ 11, \quad 30\cdot 11 = 330 \ \to\ 0.$$

However, can this behaviour be put into a general rule? Is this a trivial question? I have surmised/observed that there can be no more than nineteen zero sums in the sequence for multiples of eleven. Can you generalize?

Sebastian Hayes

$a = b$

Dear Tony,

I have the following proof which shows that a number is equal to a number which is smaller than itself.

Start with $a = b + c$. Multiply both sides by $a - b$:

$$a^2 - ab \ = \ ab + ac - b^2 - bc.$$

Move ac to the left side:

$$a^2 - ab - ac \ = \ ab - b^2 - bc.$$

Factorize:

$$a(a-b-c) \ = \ b(a-b-c).$$

Divide each side by z..., sorry, I mean $a - b - c$:

$$a \ = \ b.$$

Keith Drever

Cats

Dear Tony,

I have recently seen a roadside poster for VW with the words: 'Bora V6 Motion. Performance roadholding' beneath a picture of a car on a long, empty curve in a reasonably wide, open road with no traffic for miles. There is a fat fluffy cat asleep on the car's bonnet.

Bearing Newton's laws of motion in mind and assuming that relativistic effects can be ignored I am having difficulty in reconciling the words with the picture!

So far the only explanations that I've come up with are:

1. The cat is asleep on a car that is stationary or moving very slowly.
2. The cat has been glued on to the car or fixed in some other manner.
3. It's Schrödinger's cat.

All of the above seem highly improbable so I am seeking the help of other M500 readers in coming up with more plausible explanation.

Andrew Pettit

JRH—I remember the BMW advert for their computerized engine management system, which proudly claimed '70 mph, 0 mpg'.

Recurring runs

Susan Cook

Many integers produce a reciprocal which is a recurring decimal of the form $0.NNN\ldots$, where N is a run of digits that repeat indefinitely. For example, the reciprocal of 9 is $0.111111111111\ldots$, where the single digit 1 recurs. The run is of length 1. Similarly, $1/11 = 0.090909090909\ldots$ with a run of 09, which has run length 2, and $1/7 = 0.142857142857\ldots$ with run length 6.

What is the smallest integer whose reciprocal has run length 5?

'You are advised to avoid the A40 this morning because of delays owing to a traffic survey.' —Thames Valley Radio. [Spotted by Peter Fletcher.]

'... combine cutting-edge technology with strength and flexibility.'
—Blurb on a box of 6 cheap glass tumblers. [Ralph Hancock]

'WOMAN DIES OF DIARRHOEA AFTER ATTACK BY OWL'
—Headline in *Bangkok World*. [EK]

Eudora Welty

Eddie Kent

We are normally concerned with the wilder shores of mathematics in M500, straying occasionally into the realms of the sciences and philosophy. It thus might seem strange to see the death of a mere fiction writer noticed. But Eudora Welty will be long remembered in the world of the Internet.

She died recently, at the age of 82. Born in 1909, she was a well-loved author who began her career in 1936 with the novel *Death of a Travelling Salesman*. In 1941 her first collection of short stories appeared: *A Curtain of Green*; this, said *The Times*, is 'a very interesting collection by a gifted short-story writer'—praise indeed from the Thunderer.

One of the 17 tales was called 'Why I live at the P.O.', a monologue by a small-town postmistress on the reasons why she prefers to live at the post office, rather than suffer the persecution of her eccentric family. Like most of her work it is sad, but very funny.

In 1988 Steven Dorner wrote a freeware product that broke new ground by combining the best attributes of various emerging email technologies. He called it Eudora because, he said, he had been processing so much email he felt like a character at a post office.

Dorner and Eudora quickly became internationally known, and were soon taken over by Qualcomm. 'Eudora' is now a registered trademark of the University of Illinois Board of Trustees, and is licensed to Qualcomm Inc. So far as I know it is still free—look at qualcomm.com; this contains the full story and downloads.

Eudora Welty was amused.

Twenty-five years ago

From M500 37 & 38

Jeremy Humphries—A pack of cards is shuffled and dealt until the first black ace appears. Where it it most likely to be?

Steve Murphy—Given four distinct parallel planes show that it is always possible to construct at least one regular tetrahedron with a vertex on each plane. Show that the length of the side of any such tetrahedron is unique.

Max Bramer—There are $2N$ teams in a competition. Is it possible to arrange all possible pairings in only $2N - 1$ rounds?

Chris Pile—Suppose

$$\sum_{r=1}^{n} r^2 \;=\; \frac{1}{6}\,(n+1)(2n+1) \;=\; N^2, \qquad n,\ N \in \mathbb{Z}^+.$$

If $n = 24$ the sum is 4900, giving $N = 70$; and this solution is unique, apart from the trivial $n = N = 1$.

The problem of fitting a set of squares of sides 1 to 24 inside a square of size 70 was posed in *Scientific American* several years ago. The best arrangement omitted only the 7-square, leaving 49 unit squares uncovered. As far as I know this has not been improved upon nor shown to be minimal.

Searching for a perfect arrangement led me to consider triangular elements. An equilateral triangle of side N yields N^2 unit triangles.

Can a set of 24 equilateral triangles of sides 1 to 24 be fitted inside an equilateral triangle of side 70? If not, what is the best arrangement of a subset of the 24 triangles?

So far my best arrangement leaves 149 triangle units uncovered, omitting the 10-triangle and the 7-triangle. [See the front cover of this issue.]

Jeremy again—How many commutative groups are there?

Winter Weekend 2002

Norma Rosier

The twenty-first M500 Society WINTER WEEKEND will be held at **Nottingham University** from **Friday 4 to Sunday 6 January, 2002**.

This is an annual residential Weekend to dispel the withdrawal symptoms due to courses finishing in October and not starting again until February. It is an opportunity to get together with friends, old and new, and do some interesting mathematics. It promises to be as much fun as ever!

Ian Harrison is running it and the theme will be

Mathematics, Games and Puzzles.

Cost: £145 for M500 members, £150 for non-members. This includes accommodation and all meals from dinner on Friday to lunch on Sunday. Please send a stamped, addressed envelope for booking form to

Norma Rosier.