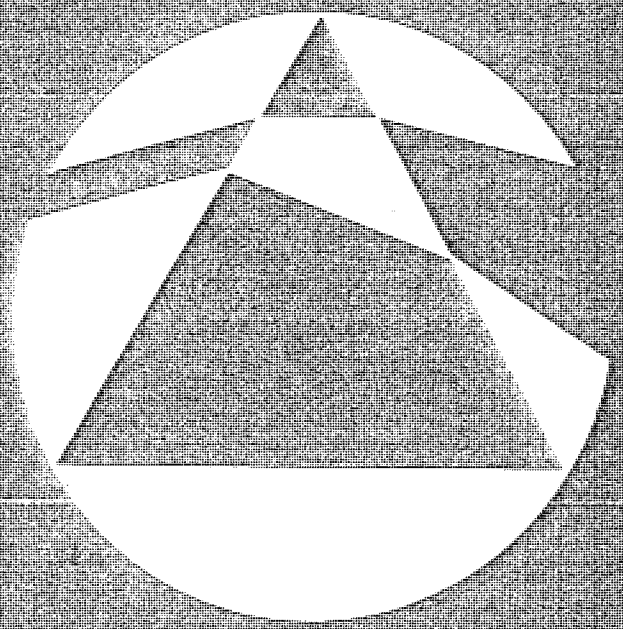
Mathematical Spectrum

1991/92
Volume 24
Number 3



A magazine for students and teachers of mathematics in schools, colleges and universities

Mathematical Spectrum is a magazine for students and teachers in schools, colleges and universities, as well as the general reader interested in mathematics. It is published by the Applied Probability Trust, a non-profit making organisation established in 1963 with the support of the London Mathematical Society. The object of the Trust is the encouragement of study and research in the mathematical sciences.

Volume 24 of *Mathematical Spectrum* will consist of four issues, of which this is the third. The first was published in September 1991, the second in November 1991 and the fourth will appear in May 1992.

Articles published in *Mathematical Spectrum* deal with the entire range of mathematical disciplines (pure mathematics, applied mathematics, statistics, operational research, computing science, numerical analysis, biomathematics). Both expository and historical material may be included, as well as elementary research and information on educational opportunities and careers in mathematics. There is also a section devoted to problems.

The Editorial Committee welcomes the submission of suitable material, including correspondence, queries and solutions to problems, for publication in *Mathematical Spectrum*. Students are encouraged to send in contributions. All correspondence about the contents should be sent to:

The Editor, Mathematical Spectrum,
Hicks Building, The University, Sheffield S3 7RH, UK

Codes (Dpeft!)

MIKE STANNETT, *University of Sheffield*

Having started out as a mathematician, the author then became interested in computing and now specialises in theoretical aspects of computer science. His main research interests include methods with which to reason about concurrent processes, and the development of non-standard computers. Outside work, he likes making strange noises on synthesizers, and is a fanatical Sheffield Wednesday supporter.

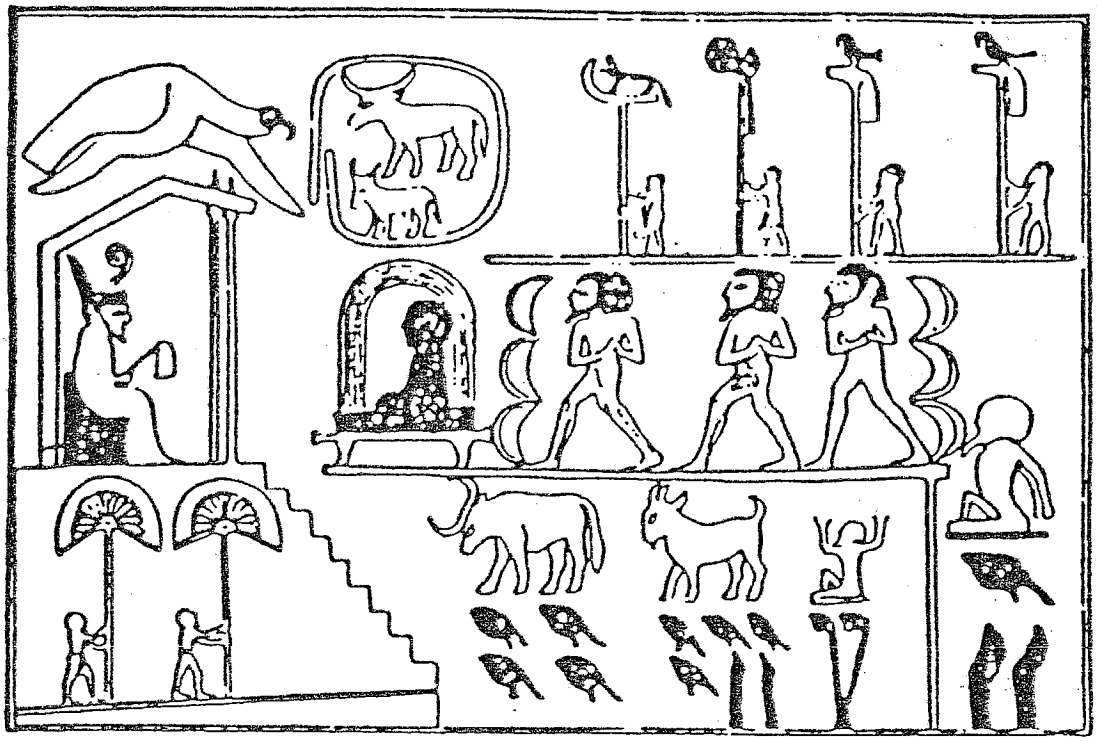
Codes are everywhere

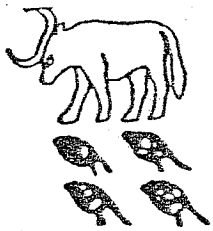
Learning a foreign language can be an infuriating business. You know those peculiar words must mean something—the problem is you just do not happen to know what they mean. And of course, the problem is exactly the same the other way around. A French person learning English for the first time has to work out what our peculiar words mean.

So, in a very real sense, language is a code. The point is, of course, that we all know what the rules are for cracking this code; after all, we spend our entire lives learning just that. But what happens if you come across a language that is entirely new to you? If you happen to know someone who speaks that language, you can ask them to tell you what things mean. But suppose that no one speaks the language any more. This is exactly what happened when people tried working out what ancient hieroglyphics mean. They knew the strange pictures must stand for something, but they did not know what. Worse still, there were no ancient Egyptians around who could translate for them. So what could they do?

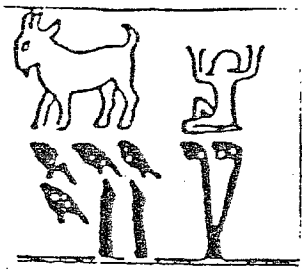
Of course, if there had only been the odd picture to go by, they would have got nowhere. For example, if all you had to go on was the picture in figure 1, how could you decide what it stood for? Is it a cow of some sort? Or perhaps the trademark of a local farmer? Or does it mean 'the time of year when the calves are born'? Obviously, you do not have enough information to come to a sensible conclusion. On the other hand, if you knew that the inscription shown in figure 2 was found on a stone macehead (and so probably gave a list of its owner's spoils of war), and if you had previously seen enough of these things to realise that some symbols definitely

Figure 1. Is it a cow?





400 000 cows



1422 000 goats

120 000 captives

Figure 2

stand for numbers, you would soon be able to work out how many cows, goats and captives he had taken.

Another thing that would certainly help would be if someone had translated a whole book for you. They might not have told you the meaning of individual words, but at least you would know roughly what they were talking about. A famous case where this happened is the Rosetta Stone, which very obligingly supplied the same text in three different languages, one of which was already known. Since people now knew roughly what the symbols were being used to say, they could start working out what individual hieroglyphs stood for. We shall soon see how these ideas can be used to crack other, secret, codes.

But why on earth should anyone ever need a secret code? The answer goes back to ancient times; Julius Caesar developed what he thought was a fiendishly clever code, to stop his enemies understanding the messages they

intercepted. (To keep things simple, we assume that Caesar wrote in English.) See if you can crack his code.

lqidpb, lqidpb, wkhb'yh doo jrw lw lq iru ph.

Hint: What could **yh** or **doo** possibly stand for? What could the two-letter words be? This is an example of a (very) simple substitution cipher. It is so called because all you do is substitute one letter for another, wherever it occurs—what could be simpler?

But what does this have to do with our hieroglyphics? Well, we can think of groups of letters like **lqidpb** as being words in another language; our job is to work out what they mean. As with hieroglyphics, the job is made much easier if we have at least a few hints to help us.

So how could we make our code more secure? That is, how could we change things so that you need more hints before you can crack the code as a whole? One way is to use a codeword. For example, suppose our codeword is *mikey*. Then we would write out the alphabet as normal, together with the word *mikey* underneath it, like this:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
m i k e y

Now we just fill in the missing letters, in alphabetical order, starting at the end of the codeword:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
q r s t u v w x z *m i k e y* **a b c d f g h j l n o p**

Now suppose you have some message that you want to write in code, such as

MATHEMATICS CAN BE FUN!

You just look up each letter in turn in the top row, and see what letter it should be replaced by. In this case, we should replace 'M' with **e**, 'A' with **q**, and so on. The final message would come out looking like this:

eqgxueqgzsf sqy ru vhy!

To crack this code, you need two bits of information. First of all, you need to know that the codeword is *mikey*. You also need to know that I wrote *mikey* starting under the letter 'J'. Starting somewhere else would have given me a different code.

But suppose you did not have these two bits of information, or suppose the code was a lot more random, like

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
e n j w s l i v a x b q m r u f z t o p c y h k d g

We shall now see how to cope with these more complex codes.

Cracking a code

You will probably be quite surprised how difficult it can be to crack such a simple type of code. Nonetheless, it can be done. Fortunately there is some information that we have not yet used: we know what language the original uncoded message is in. It is helpful to know this because some letters in English (or French, or German, or whatever) are much more common than others. In written English, the frequencies with which different letters are used are well known (see table 1). You can see from the table that the commonest letter is 'E', then 'T', then 'A', 'I', and so on.

Table 1. Percentage frequency of letters in English

A	B	C	D	E	F	G	H	I	J	K	L	M
7.7	1.7	3.2	4.2	12.0	2.4	1.7	5.0	7.6	0.4	0.7	4.2	2.4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
6.7	6.7	2.0	0.5	5.9	6.7	8.5	3.7	1.2	2.2	0.4	2.2	0.2

How does this help us? Well, remember how the encoding method works; we always replace a letter in the message with the letter underneath it in the table. So if we always replace 'E' with **j**, say, then we should expect 12% of all the characters in the message to be **j**'s. To put it another way, if we count the letters in some other encoded message, and roughly 12% of them happen to be **j**, then we should have good grounds for supposing that **j** stands for 'E' in that particular code.

Unfortunately, this process only really helps when it comes to finding 'E'—all the other letter frequencies are too close together, and it is easy to get letters mixed up. Still, it gives us a start. Here is an example.

Message/13/Oct/90/Banknet.mps
uwdivrwk zcclgliev tzqdf uz ywdvdsu i vudwelsb gwlvlv uzfik hk vlbsieelsb upiu updk iwd ywdyiwdf uz wilvd lsudwdvu wiudv uz ywzudgu vudwelsb.

How often do the different letters appear in this message? A quick count gives us table 2. It seems quite likely that 'E' is represented by either **d** or **u**. But how can we tell which of these it is? From the figures in the table,

Table 2. Percentage frequency of letters in message

a	b	c	d	e	f	g	h	i	j	k	l	m
0	2.9	1.9	12.5	3.8	2.9	1.9	1.0	9.6	0	3.8	8.7	0
n	o	p	q	r	s	t	u	v	w	x	y	z
0	0	1.9	1.0	1.0	4.8	1.0	12.5	9.6	10.6	0	2.9	5.8

there is no easy way to decide—all we can do is try both possibilities, and see which one looks more reasonable. Let us start with 'E' = **d**. We go through the message, replacing every **d** with a corresponding 'E', like this:

> **uwEivrwk zcclgliev tzqEf uz ywEqEsu i vuEwelsb gwlvlv uzfik hk vlbsieelsb upiu upEk iwE ywEyiwEf uz wilvE lsuEwEvu wiuEv uz ywzuEgu vuEwelsb.**

At the same time, we update our 'key':

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
d

Since it is not very safe to use the frequencies to guess any of the other letters, we have to find some other technique. In the message above we have been given some extra help, because we know where the different words start and finish. In particular, we know that **i** is a one-letter word. The most likely choice is therefore that **i** stands for 'A'. So we can write this in as well:

> **uwEAvrwk zcclglAev tzqEf uz ywEqEsu A vuEwelsb gwlvlv uzfAk hk vlbsAeelsb upAu upEk AwE ywEyAwEf uz wAlvE lsuEwEvu wAuEv uz ywzuEgu vuEwelsb.**

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
i d

This, of course, is guesswork, but then most of code-cracking is! Still, we are getting somewhere. The three-letter sequence 'AwE' could be one of many words, but how can we decide which? Looking at the letter frequencies, it is quite likely that it should be 'ATE' because **w** occurred so frequently. But, on the other hand, the word 'ARE' is a much more likely candidate. As always, all we can do is to choose one and see what happens, so I shall choose 'ARE' and replace **w** with 'R'.

> **uREAvrRk zcclglAev tzqEf uz yREqEsu A vuERelsb gRlvlv uzfAk hk vlbsAeelsb upAu upEk ARE yREyAREf uz RAlvE lsuEREvu RAuEv uz yRzuEgu vuERelsb.**

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
i d w

You may now feel confident enough to guess some more: what about the two-letter word **uz** that occurs three times? It ought to be something like 'AT', 'OF', 'IN', or 'TO'. But it cannot be 'AT', because we have already allocated the letter 'A'. What about the others? Look at the word **vuERelsb**. What would this become if **uz** was 'AT'? We should end up with the letters 'AER' in the middle of the word, which is very unlikely.

Similarly, if **uz** was 'OF', we should get 'OER', which is also unlikely. On the other hand, interpreting **uz** as 'TO' is at least plausible, since we would end up with 'TER', which is quite a common letter sequence. So let us try it:

TREAvrRk OcclglAev tOqEf TO yREqEsT A vTERelsb gRlvlv TOfAk hk vlbsAeelsb TpAT TpEk ARE yREyAREf TO RAlvE lsTEREvT RATEv TO yROTEgT vTERelsb.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
i				**d**										**z**			**w**		**u**						

Working out the rest of the message is now quite straightforward. Whatever **y** stands for, it must fit into both **yREyAREf** and **yROTEgT**. This means that it must be 'P', in which case it is easy to see from PREPAREf that **f** is 'D'. Similarly, by looking at **lsTEREvT RATEv**, it is obvious that **v** stands for 'S', and that the first word must be INTEREST. I'll leave the rest to you!

You would be forgiven for thinking that this is all a bit of a fraud, and that there ought to be a more scientific way of doing things. There is, of course, but in the long run it really does all come down to guesswork at this level.

And finally ...

'ZWLU RF ERLU IUWOF BTZUO MCWS YUJ. RE R WZZ YUJ'F WNU MB XUS'F, WSZ MCUS OULUOFU MCU BOZUO BE MCU ZRNRMF, R NUM ZWLU'F WNU. ZWLU RF IBGSNUO MCWS XUS'.

How old is Jez if Ben is fourteen?

The 1992 Puzzle

A reader, Mark Lighterman of Miami, Florida, has anticipated our annual puzzle, which is to express the numbers 1 to 100 in terms of digits of the year in order, using only $+$, $-$, $\times$, $\div$, $\sqrt{}$, ! and concatenation (i.e. constructing the number 19 from 1 and 9, for example). As an illustration, Mark gives $43 = 1+(\sqrt{9})!(9-2)$ (one which defeated the editor!). Mark failed with four of the numbers: 69, 75, 91 and 93.

Factorising Polynomial Pairs

K. R. S. SASTRY, *Box 21862, Addis Ababa, Ethiopia*

The author's name is familiar to readers of *Mathematical Spectrum*. Here he shows how the very familiar idea of quadratic factorisation leads to interesting new questions that demand different techniques for their solution. In the process he discovers a relationship between a type of quadratic polynomial and generating self-median triangles.

1. The basic problem

Look at the following pairs of quadratic polynomials:

$$\text{(i)}\quad x^2+8x+12, \qquad x^2+8x+15;$$

$$\text{(ii)}\quad 2x^2+3x-2, \qquad 2x^2+3x+1;$$

$$\text{(iii)}\quad 5x^2+22x+21, \qquad 5x^2+22x+24.$$

They all factorise over the integers. The curious fact about them is that in each pair the two polynomials differ by the same constant, in this case 3. Naturally one wonders if there is an infinity of such pairs. This is, in fact, the case quite generally, as we shall show. To this end let us state the problem as follows.

> Determine the set of integers $\{(a, b, c, d)\}$ so that both members of the polynomial pair ax^2+bx+c and $ax^2+bx+c+d$ factorise over the integers. (*)

The construction which we shall describe below gives a partial solution only to this problem.

Now the factorisation of a polynomial such as $5x^2+22x+21$ into $(x+3)(5x+7)$ is equivalent to having rational roots to the corresponding equation $5x^2+22x+21 = 0$. This in turn is equivalent to having its discriminant a perfect square. (The discriminant of ax^2+bx+c is b^2-4ac.) Hence the polynomial pair in (*) factorises over the integers if and only if there exist integers m and n (negative, zero or positive) such that

$$b^2-4ac = m^2 \quad \text{and} \quad b^2-4a(c+d) = n^2. \tag{1}$$

Our immediate aim is to determine the coefficients a, b, c and d in terms of the parameters m and n. The observation that $m^2-n^2 = 4ad$ is an even integer implies that m and n are either both odd or both even and yields one set of values $a = \frac{1}{2}(m+n)$, $d = \frac{1}{2}(m-n)$. Put $a = \frac{1}{2}(m+n)$ in $b^2-4ac = m^2$ and obtain

$$c = \frac{b^2-m^2}{2(m+n)} \qquad (m+n \neq 0).$$

(If $m+n = 0$ then $a = 0$ and ax^2+bx+c reduces to a first-degree polynomial.) We should choose the value of b so that the resulting c is an integer. If $b = \pm m+\lambda(m+n)$ then

$$c = \tfrac{1}{2}\lambda^2(m+n) \pm \lambda m$$

will be an integer for each integer λ. Also if $\beta = \pm n+\lambda(m+n)$ then

$$c = \tfrac{1}{2}\lambda^2(m+n) \pm \lambda n - \tfrac{1}{2}(m-n)$$

will be an integer for each integer λ. So we have

$$\begin{aligned} a &= \tfrac{1}{2}(m+n), \\ b &= \pm m+\lambda(m+n) \quad \text{or} \quad \pm n+\lambda(m+n), \\ c &= \tfrac{1}{2}\lambda^2(m+n) \pm \lambda m \quad \text{or} \quad \tfrac{1}{2}\lambda^2(m+n) \pm \lambda n - \tfrac{1}{2}(m-n), \\ d &= \tfrac{1}{2}(m-n). \end{aligned} \tag{2}$$

Since $a = \frac{1}{2}(m+n)$ and $d = \frac{1}{2}(m-n)$ yield $m = a+d$ and $n = a-d$, we see that b and c are expressible in terms of a and d:

$$\begin{aligned} b &= \pm(a+d)+2\lambda a \quad \text{or} \quad \pm(a-d)+2\lambda a, \\ c &= a\lambda^2 \pm (a+d)\lambda \quad \text{or} \quad a\lambda^2 \pm (a-d)\lambda - d, \end{aligned} \tag{3}$$

where $a \neq 0$, d and λ are any integers. The reader should verify that b^2-4ac and $b^2-4a(c+d)$ are perfect squares. As an illustration, let us take $a = 4$, $d = 5$ and $\lambda = 3$ in (3). This produces

$$b = 33, 15, 23, 25, \qquad c = 63, 9, 28, 34$$

and the factorising polynomial pairs

$$4x^2+33x+63, \quad 4x^2+33x+68; \qquad 4x^2+15x+9, \quad 4x^2+15x+14;$$
$$4x^2+23x+28, \quad 4x^2+23x+33; \qquad 4x^2+25x+34, \quad 4x^2+25x+39.$$

2. A limit to the factorisation chain

Curiosity extends the basic problem (*) and asks: how many steps can we climb up this factorisation ladder? The answer is: not many. To see this, consider the chain of quadratic polynomials ax^2+bx+c, $ax^2+bx+c+d$, $ax^2+bx+c+2d$, ..., each of which factorises over the integers. This is possible if and only if we have integers m_1, m_2, m_3, ... such that

$$b^2-4ac = m_1^2, \quad b^2-4a(c+d) = m_2^2, \quad b^2-4a(c+2d) = m_3^2, \quad \ldots. \tag{4}$$

Here the left-hand-side members of (4) form an arithmetic progression

with $-4ad$ as the common difference. Therefore the corresponding members $m_1^2, m_2^2, m_3^2, \ldots$ on the right-hand side should also form an arithmetic progression with the same common difference. However, it is known that not more than three squares can be in arithmetic progression (reference 2, page 440). This leaves us with only three equations to consider:

$$b^2-4ac = m_1^2, \qquad b^2-4a(c+d) = m_2^2, \qquad b^2-4a(c+2d) = m_3^2.$$

One set of solutions

$$m_1 = p^2+2pq-q^2, \qquad m_2 = p^2+q^2, \qquad m_3 = p^2-2pq-q^2$$

(reference 2, page 435) yields m_1^2, m_2^2 and m_3^2 in arithmetic progression. (Verify this claim!) If we take

$$a = \tfrac{1}{2}(m_1+m_2) = p^2+pq \quad \text{then} \quad d = \tfrac{1}{2}(m_1-m_2) = pq-q^2,$$

and b and c are as in (3). For instance, $p = 2$, $q = 1$ and $\lambda = -1$ produce the following triplets:

$$\begin{array}{lll} 6x^2-5x-1, & 6x^2-5x, & 6x^2-5x+1; \\ 6x^2-19x+13, & 6x^2-19x+14, & 6x^2-19x+15; \\ 6x^2-7x, & 6x^2-7x+1, & 6x^2-7x+2; \\ 6x^2-17x+10, & 6x^2-17x+11, & 6x^2-17x+12. \end{array}$$

At this point it is instructive to recall the definition of a self-median triangle: a triangle in which the sides are proportional to the medians (reference 3). For a triangle to be self-median, the squares of its sides should be in arithmetic progression. Therefore, when the above numbers m_1, m_2 and m_3 can form a triangle then it will be a self-median triangle. Here is a nice connection between generating factorising quadratic triplets in arithmetic progression and generating the self-median triangles.

3. Related questions

The basic problem (*) raises analogous but more interesting questions. In this section we still stay with the quadratics. In section 5 we discuss higher-degree polynomial pairs that factorise over the integers.

Firstly we notice that the problem of determining the factorising polynomial pair ax^2+bx+c and $(a+d)x^2+bx+c$ is no different because this pair factorises over the integers if and only if the corresponding pair cx^2+bx+a and $cx^2+bx+a+d$ does.

The next problem of determining the factorising pair ax^2+bx+c and $ax^2+(b+d)x+c$, intriguingly, requires a different solution strategy. We now need integers m and n such that

$$b^2-4ac = m^2 \quad \text{and} \quad (b+d)^2-4ac = n^2.$$

This gives the relationship

$$(b+d)^2+m^2 = b^2+n^2 \tag{5}$$

to be satisfied by b, d, m and n. Therefore, to determine these elements we need a number such as 65 that can be expressed as the sum of two integral squares in two distinct ways:

$$8^2+1^2 = 65 = 7^2+4^2.$$

Then we put $b+d = 8$, $m = 1$, $b = 7$ and $n = 4$, and obtain $d = 1$. From $b^2-4ac = m^2$ we get $ac = 12$. Choosing $a = 6$ and $c = 2$ produces the factorising pair $6x^2+7x+2$ and $6x^2+8x+2$. Note that we could also equate $b+d = -1$, $m = 8$, $b = 4$ and $n = -7$, and obtain a solution pair $12x^2+4x-1$ and $12x^2-x-1$. A more general solution of (5) can be obtained from the identity

$$(pq+rs)^2+(ps-qr)^2 = (pq-rs)^2+(ps+qr)^2. \tag{6}$$

Proceeding as in the numerical illustration, by equating

$$b+d = pq+rs, \qquad m = ps-qr, \qquad b = pq-rs, \qquad n = ps+qr$$

we obtain

$$b = pq-rs, \qquad d = 2rs, \qquad m = ps-qr, \qquad n = ps+qr,$$
$$4ac = (p^2-r^2)(q^2-s^2). \tag{7}$$

Here either p and r or q and s should have the same parity to produce an integral value for ac. If we let $p = 3$, $q = 3$, $r = -7$ and $s = 1$ in (7) then we obtain $b = 16$, $d = -14$, $m = 24$, $n = -18$ and $ac = -80$. Taking $a = 16$ and $c = -5$, we have the factorising pair $16x^2+16x-5$ and $16x^2+2x-5$. We now leave the very interesting and indeed very challenging problem of determining the sequence of factorising polynomials (over the integers)

$$ax^2+bx+c, \quad ax^2+(b+d)x+c, \quad ax^2+(b+2d)x+c, \quad \ldots \quad (c \neq 0).$$

(If $c = 0$, it is a trivial problem.) The example

$$x^2+27x+180, \qquad x^2+28x+180, \qquad x^2+29x+180$$

shows that such a factorising triplet certainly exists. Can this sequence of factorising polynomials have more than three members? Are there geometric problems whose solutions are related to the determination of such sequences? These open problems are worth investigating.

4. Multigrades

Certain sets of numbers have curious properties. For example, the sets of numbers $\{2,5,14\}$ and $\{9,12\}$ have their sums as well as the sums of

their squares equal, i.e.

$$2^n+5^n+14^n = 9^n+12^n \quad (n = 1,2).$$

This relationship is called *bigrade* and is denoted by the symbol

$$2,5,14 \overset{2}{=} 9,12.$$

Analogously, we have the trigrade

$$1,4,5,5,6,9 \overset{3}{=} 2,3,3,7,7,8$$

because

$$1^n+4^n+5^n+5^n+6^n+9^n = 2^n+3^n+3^n+7^n+7^n+8^n \quad (n = 1,2,3).$$

In general such relationships as are shown in the above examples that hold simultaneously for several powers are called *multigrades*. An interesting account of multigrades is given in reference 1, pages 162–165. Special multigrades of the type

$$\alpha_1,\alpha_2,\ldots,\alpha_n \overset{n-1}{=} \beta_1,\beta_2,\ldots,\beta_n,$$

that is, having n integers on each side together with

$$\alpha_1^i+\alpha_2^i+\ldots+\alpha_n^i = \beta_1^i+\beta_2^i+\ldots+\beta_n^i \quad (i = 1,2,\ldots,n-1) \tag{8}$$

will be of interest to us. We shall make use of them in the next section. In the meantime the reader is advised to verify the bigrades

$$\alpha_1,\alpha_2,\alpha_3 \overset{2}{=} \beta_1,\beta_2,\beta_3,$$

where

$$\text{(i)}\ \ (\alpha_1,\alpha_2,\alpha_3) = (p+q,r,s), \qquad (\beta_1,\beta_2,\beta_3) = (p,q,r+s), \tag{9}$$

in which $pq = rs$, due to A. Cunningham (reference 2, page 706), and

$$\text{(ii)}\ \ (\alpha_1,\alpha_2,\alpha_3) = (pq+rs,pr,qs), \qquad (\beta_1,\beta_2,\beta_3) = (pr+qs,pq,rs), \tag{10}$$

due to R. W. D. Christie (reference 2, page 706), and the trigrade

$$\alpha_1,\alpha_2,\alpha_3,\alpha_4 \overset{3}{=} \beta_1,\beta_2,\beta_3,\beta_4,$$

where

$$\begin{aligned}(\alpha_1,\alpha_2,\alpha_3,\alpha_4) &= (p,p+q-2r,p+2q+r,p+3q-r),\\ (\beta_1,\beta_2,\beta_3,\beta_4) &= (p+3q,p+q+r,p-r,p+2q-2r),\end{aligned} \tag{11}$$

due to C. Bisman (reference 2, page 709).

5. Factorising polynomial pairs in general

The problem of determining pairs of polynomials

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \quad \text{and} \quad P(x)+d \quad (n > 2)$$

such that each of them factorises into n linear factors over the integers is, surprisingly, linked to the problem of determining multigrades of the type described by (8). We shall show this interdependence in the case of a cubic pair. Similar, but tedious, methods prove the general case.

To begin with, let us suppose that the leading coefficient a_3 is equal to 1. Later on, by means of an example, we shall show the method of obtaining the desired pair of polynomials in which the leading coefficient is not necessarily 1. Suppose then, that we have the factorising cubic pair

$$\begin{aligned} P(x) &= x^3 + a_2x^2 + a_1x + a_0 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3), \\ P(x)+d &= x^3 + a_2x^2 + a_1x + a_0 + d = (x-\beta_1)(x-\beta_2)(x-\beta_3). \end{aligned} \tag{12}$$

Multiplying out the factors and equating the coefficients of like powers of x yields

$$\begin{aligned} \alpha_1+\alpha_2+\alpha_3 &= -a_2 = \beta_1+\beta_2+\beta_3, \\ \alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1 &= a_1 = \beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1, \\ \alpha_1\alpha_2\alpha_3 - \beta_1\beta_2\beta_3 &= d. \end{aligned} \tag{13}$$

Now

$$\begin{aligned} \alpha_1^2+\alpha_2^2+\alpha_3^2 &= (\alpha_1+\alpha_2+\alpha_3)^2 - 2(\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_1) \\ &= (\beta_1+\beta_2+\beta_3)^2 - 2(\beta_1\beta_2+\beta_2\beta_3+\beta_3\beta_1) \\ &= \beta_1^2+\beta_2^2+\beta_3^2, \end{aligned}$$

so that

$$\alpha_1, \alpha_2, \alpha_3 \overset{2}{=} \beta_1, \beta_2, \beta_3 \tag{14}$$

is a bigrade. Conversely, starting with a known bigrade (14) we can form the factorising cubic pair (12). In particular, Cunningham's bigrade (9) leads to

$$P(x) = [x-(p+q)](x-r)(x-s), \qquad P(x)+d = (x-p)(x-q)[x-(r+s)],$$

where $pq = rs$ and $d = pq(p+q-r-s)$. Letting $p = 6$, $q = 1$, $r = 3$ and $s = 2$, so that $pq = rs = 6$, we get the polynomial pair

$$P(x) = (x-7)(x-3)(x-2), \qquad P(x)+12 = (x-6)(x-1)(x-5).$$

The reader can form the factorising cubic pairs $P(x)$ and

$P(x)+pqrs(p-s)(q-r)$ using Christie's bigrade (10) and the quartic pairs $P(x)$ and $P(x)-6qr(q+r)(q-r)$ using the trigrade in (11). Perhaps the most spectacular factorising pair is the eighth-degree one that we can form from Tarry's heptagrade (reference 2, page 710):

$$P(x) = (x-1)(x-5)(x-10)(x-24)(x-28)(x-42)(x-47)(x-51),$$

$$P(x)+d = (x-2)(x-3)(x-12)(x-21)(x-31)(x-40)(x-49)(x-50),$$

where $d = 1210\,809\,600$.

We observe that the bigrades (9) and (10) and the trigrade (11) are algebraic identities. In particular, they hold when p, q, r and s are rational numbers that are not necessarily integers. This observation can be used to obtain a factorising pair $P(x)$ and $P(x)+d$ over the rationals. These can then be modified to obtain a desired pair over the integers in which the leading coefficient is not necessarily 1. As an illustration, let $p = 1$, $q = \frac{1}{2}$ and $r = \frac{1}{3}$ in (11). Then

$$(\alpha_1,\alpha_2,\alpha_3,\alpha_4) = (1, \tfrac{5}{6}, \tfrac{7}{3}, \tfrac{13}{6}), \quad (\beta_1,\beta_2,\beta_3,\beta_4) = (\tfrac{5}{2}, \tfrac{11}{6}, \tfrac{2}{3}, \tfrac{4}{3}), \quad d = -\tfrac{5}{36}.$$

So

$$P(x) = (x-1)(x-\tfrac{5}{6})(x-\tfrac{7}{3})(x-\tfrac{13}{6}), \quad P(x)-\tfrac{5}{36} = (x-\tfrac{5}{2})(x-\tfrac{11}{6})(x-\tfrac{2}{3})(x-\tfrac{4}{3}).$$

The polynomial pair just obtained is over the rationals. If we multiply each of these polynomials by 108, the result will be

$$\begin{aligned} \pi(x) &= (x-1)(6x-5)(3x-7)(6x-13) \\ &= 108x^4-684x^3+1527x^2-1406x+455, \\ \pi(x)-15 &= (2x-5)(6x-11)(3x-2)(3x-4) \\ &= 108x^4-684x^3+1527x^2-1406x+440, \end{aligned}$$

a factorising quartic pair over the integers.

6. Concluding remarks

Because of the nature of the problems we have discussed and the solution techniques employed to solve them, we have not obtained complete solutions at any of the stages (2), (3), (4), (7), (9), (10) or (11). Other multigrades suitable for generating factorising pairs of polynomials over the integers can be found on pages 705 to 713 in reference 2. Several interesting problems suggest themselves in several directions. All that remains now is to wish readers success in any further investigation of curious polynomial pairs, triplets, ...

References

1. Albert H. Beiler, *Recreations in the Theory of Numbers* (Dover, New York, 1966).

2. L. E. Dickson, *History of the Theory of Numbers*, Volume II (Chelsea, New York, 1971).
3. K. R. S. Sastry, Self-median triangles, *Mathematical Spectrum* **22** (1989/90), 58–60.

P_k-Sets

JOSEPH MCLEAN, *Computer Services Department, Strathclyde Region*

The author obtained an M.Sc. at the University of Glasgow, after which he was a research assistant in the Department of Computer Science at the University of Strathclyde. He is now an analyst and programmer in the Computer Services Department of Strathclyde Region. His main mathematical interest is in number theory.

The article by Chris Nash in *Mathematical Spectrum* Volume 22 Number 1 reminded me of a related paper (reference 1) in which we find the following definition:

> A P_k-set P of length n is a set $P = \{x_1, \ldots, x_n\}$ of n distinct positive integers, where $n \geq 2$, such that, for every pair i, j with $i \neq j$, $x_i x_j + k$ is a perfect square.

For example,

$$\{1, 2, 7\} \text{ is a } P_2\text{-set of length 3;}$$

$$\{1, 5, 10\},\ \{1, 2, 5\} \text{ and } \{2, 5, 13\} \text{ are } P_{-1}\text{-sets of length 3;}$$

$$\{1, 3, 8, 120\} \text{ is a } P_1\text{-set of length 4.}$$

Further, a P_k-set P of length n is said to be *extendible* if there exists a positive integer x not in P such that $P \cup \{x\}$ is also a P_k-set.

Reference 1 is largely taken up with proofs that certain types of P_k-set of length 3 cannot be extended. For instance, it is proved that, if $k \equiv 2 \pmod 4$, then a P_k-set of length 3 is not extendible. Many of the proofs use simple congruence and parity arguments. However, particular results, such as the non-extendibility of the P_{-1}-set $\{1, 5, 10\}$, require more complex arguments using Diophantine approximation (with which I am only vaguely familiar) and the aid of a computer to calculate certain real numbers to a large number of decimal places.

A more traditional argument in Diophantine analysis is used in another paper (reference 2) to prove that the P_2-set $\{1, 2, 7\}$ is not extendible.

However, the proof is quite elaborate and it is surprising that the following simple proof, which I came upon easily, was overlooked.

Theorem. The P_2-set $P = \{1, 2, 7\}$ is not extendible.

Proof. Suppose, to the contrary, that P can be extended, by t say. Then by definition we have

$$t+2 = a^2, \tag{1}$$

$$2t+2 = b^2, \tag{2}$$

$$7t+2 = c^2 \tag{3}$$

for some positive integers a, b and c. Substituting equation (1) into (2) and (3), respectively, we obtain

$$2a^2-2 = b^2, \tag{4}$$

$$7a^2-12 = c^2. \tag{5}$$

In equation (4), if a is even then $a^2 \equiv 0 \pmod 4$ and so $b^2 \equiv 2 \pmod 4$, a contradiction. Thus a must be odd. Similarly, in equation (5), if we suppose that a is odd, then $a^2 \equiv 1 \pmod 4$ and so $c^2 \equiv 3 \pmod 4$, again a contradiction, and so a must be even. Since is is obviously absurd that a is both odd and even, the original supposition that P is extendible is false. Hence the result.

In a quick check, I verified that the P_1-set $\{1, 8, 15\}$ is extendible by 528 and the P_4-set is extendible by 96. Brown (reference 1) proved that the P_{-1}-set $\{1, 2, 5\}$ is not extendible. Lastly, apart from the fact that it has been proved that the P_1-set $\{1, 3, 8, 120\}$ cannot be extended, I know of no results concerning P_k-sets of length 4.

References

1. Ezra Brown, Sets in which $xy+k$ is always a square, *Math. Comp.* **45** (1985), 613–620.

2. N. Thamotherampillai, The sets of number $\{1, 2, 7\}$, *Bull. Calcutta Math. Soc.* **72** (1980), 195–197.

The great Indian mathematician Ramanujan was challenged when he was 15 to solve the simultaneous equations

$$\sqrt{x}+y = 7, \qquad \sqrt{y}+x = 11.$$

He worked it out in half a minute. Can you find the solution?

From *The Man who Knew Infinity, a Life of the Genius Ramanujan* by Robert Kanigel (Scribners, 1991).

The Ocean Challenge

A. J. ELLIOTT, *University of Wales, Bangor*

Alan Elliott studied mathematics at Sheffield before gaining his Ph.D. in oceanography at Liverpool. He is now a reader in oceanography at the Marine Science Laboratories, Menai Bridge, where he is the director of the Unit for Coastal and Estuarine Studies.

There is little doubt that the most challenging problems to face society during the next century will involve aspects of climatic change and population growth. For example, if carbon dioxide levels continue to rise in the atmosphere, it is predicted that global warming due to the greenhouse effect will increase mean air temperatures by up to two degrees Celsius and raise mean sea levels by up to 0.5 metres. This would cause dramatic changes in rainfall patterns which would lead to crop failures, and many low-lying regions in the world would be submerged by the flood waters that are expected to accompany the increased frequency of severe storms.

The oceans play a crucial role in climate control since they act as the thermal flywheel because of their large heat capacity. A column of sea water only 2.5 metres deep can hold as much heat as a column of air extending from the sea surface to the upper limit of the atmosphere. This large heat-carrying capacity of the oceans is due to the fact that the specific heat and density of water are much greater than those of air; and it is enhanced by the depth of the ocean basins (typically greater than 5000 metres). As a result of the thermal inertia of the oceans, many climate experts insist that it is too soon to look for evidence of global warming as a result of the increasing levels of carbon dioxide in the atmosphere because it will take 50–100 years before sea temperatures will be influenced by the greenhouse effect. Since sea temperatures control the climate, the experts argue that the anomalous weather in recent years should be explained in terms of natural variability and not interpreted as a symptom of global warming.

Oceanographers can expect to play an important role in resolving such problems during the next few decades. The study of ocean circulation received an impetus in the 1960s when it was discovered that the mean (i.e. large-scale) currents are not slow and steady but are characterised by variations with a short time scale. In addition, the oceans are now known to be filled with small-scale regions of high current energy called 'eddies'. In the atmosphere such features are well known; they are the high- and low-pressure regions that give rise to our 'weather'. As in the atmosphere, most of the heat that is carried by ocean currents is transported by the eddies and not by the mean circulation. Figure 1 shows a satellite picture

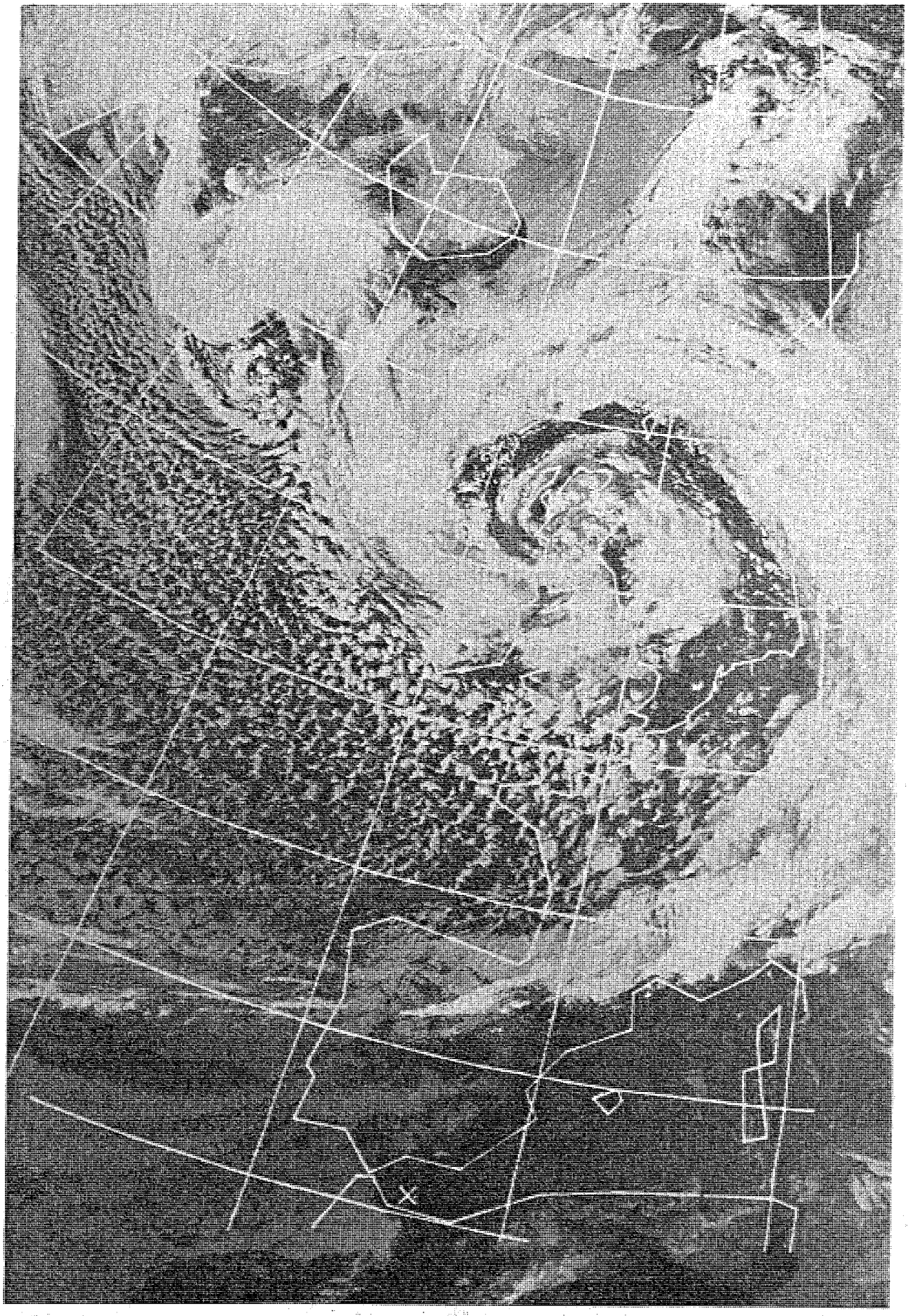


Figure 1. A satellite picture of the atmosphere

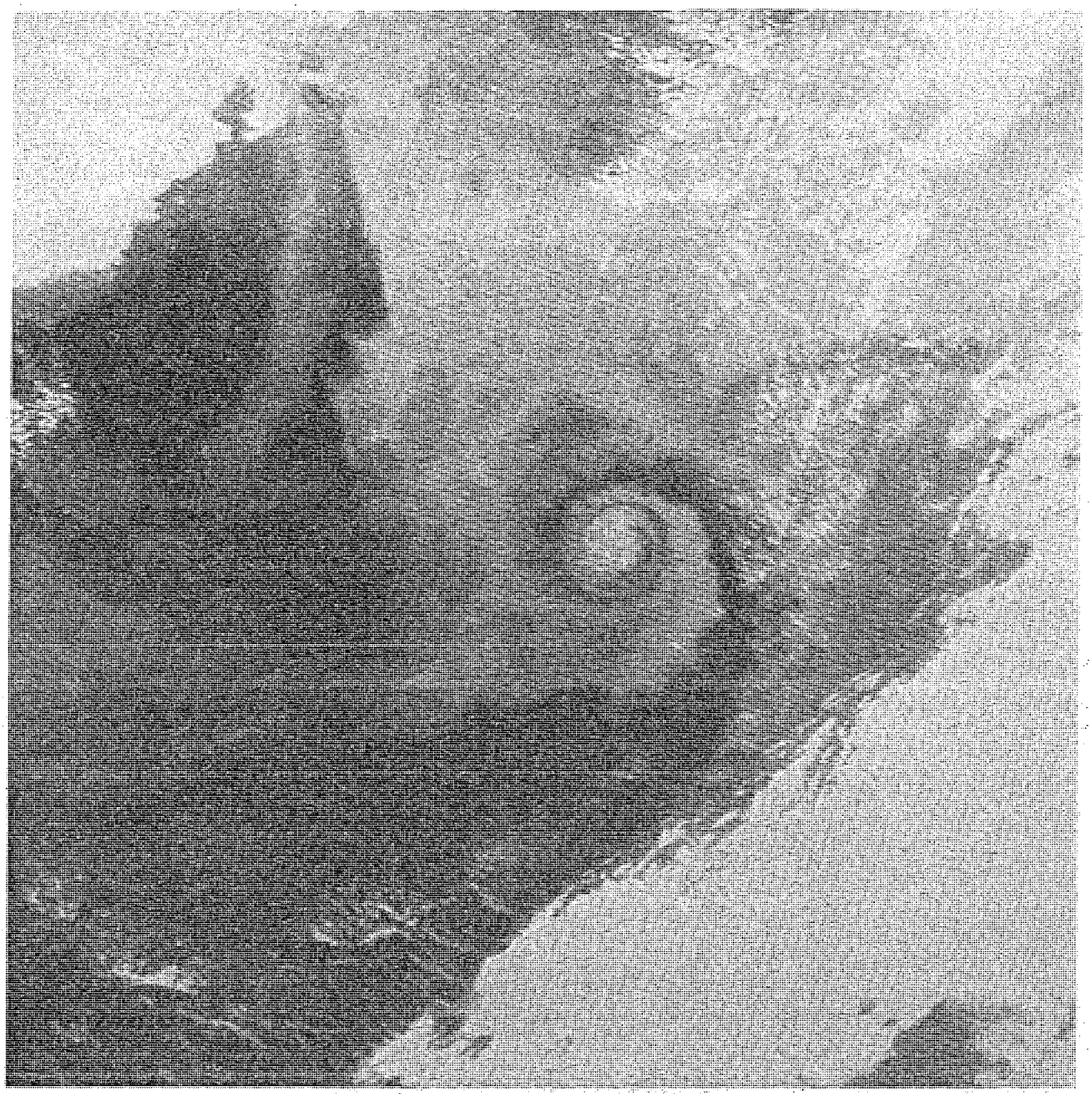


Figure 2. A satellite picture of an ocean eddy

of the atmosphere, revealing the distinctive pattern of a low-pressure system located over Britain. For comparison, Figure 2 shows a satellite picture of an ocean eddy in the Bay of Biscay. The similarity is apparent. The main differences between the two features are their space and time scales; atmospheric depressions are larger and evolve more rapidly than their oceanic counterparts. However, their dynamics are largely equivalent, and an understanding of the transport of heat by ocean eddies and of the interaction between the ocean and atmosphere is essential if predictions of climatic change are to be made.

The dynamic and thermodynamic equations that describe the momentum and heat balance of the oceans are complicated and cannot be solved analytically. They are therefore solved numerically, using sophisticated

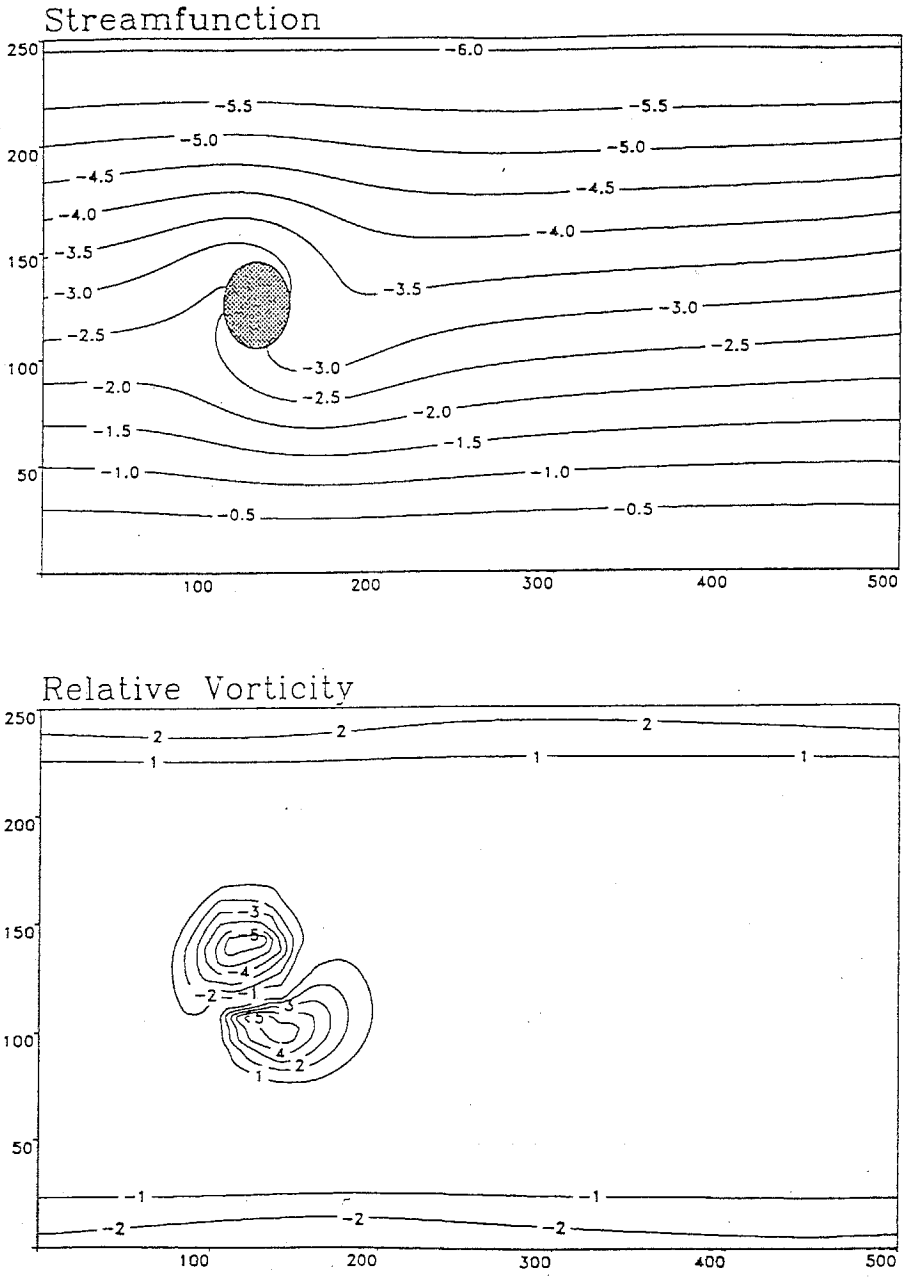


Figure 3. A mean flow crossing a sea mount

computer programs that require supercomputers for their execution. Most of the numerical techniques that are used have been developed during the past 20 years by mathematicians working in meteorological research centres. Oceanographers are thus fortunate since they can build on the earlier work of the meteorologists. However, the ocean problem is complicated by the irregular shapes of the ocean boundaries, since unlike the atmosphere the oceans are separated by the continental land masses and intersected by mid-oceanic ridges.

Mathematicians are actively involved in research directed at improving the numerical simulation of ocean circulation and the coupling between the ocean and the atmosphere. Since the numerical methods provide only

approximate solutions to the governing equations, much effort is directed towards improving the accuracy of the solutions. In particular, there has been much progress in recent years towards developing methods that are self-correcting in circumstances when large errors are likely to be generated by the numerical scheme. (One example of this is the flux correction method used to remedy the unrealistic diffusion that occurs when simulating the transport of heat by an ocean current.) In my own group a graduate mathematician has been looking at the effect that a sea mount can have on an ocean current. (A sea mount is rather like a mountain that rises from the sea bed to within close proximity of the sea surface.) It is thought that such features can have a significant influence on an ocean current by generating vertical and horizontal mixing and we are investigating ways in which such features can be simulated numerically. Figure 3 shows a mean flow moving from west to east and demonstrates how it meanders as it crosses a sea mount. The calculations were made on a Cray supercomputer and the figure was produced using a powerful graphics workstation. As the flow passes the sea mount it rotates slightly; this has the effect of raising the sea level on one side of the sea mount and depressing it on the other side. As a consequence, two patches of water of slightly different temperature are formed above the sea mount due to vertical mixing of the surface water with the cooler water beneath. Such eddy-like features are sometimes revealed near islands by satellite images, and our work is aimed at evaluating the effects of these features on both the dynamics of the mean flow and on the resulting temperature distributions.

Above all, oceanography is an observational science; mathematicians who work in oceanographic laboratories can expect to spend time at sea on research ships. Research cruises typically last 2–4 weeks, during which time data are recorded on computer systems that are interfaced to instruments which are towed or lowered through the water. The instruments, which record the pressure, temperature, salinity and other chemical properties of the water, sample several times each second; this means that large amounts of data are collected. Part of the challenge lies in processing and analysing these large data sets so that the underlying physical structure of the oceans can be revealed. Some instruments (for example, those that measure ocean currents) are left in the sea attached to fixed moorings so that long records are collected at selected positions. More recently, satellite images have shown details of the ocean circulation that were previously unsuspected. Combined with more conventional measurements, these present the oceanographer with the data that are required to test theoretical ideas and computer models.

In summary, therefore, oceanography presents many challenging problems, and the environmental sciences can provide a rewarding career for young mathematicians.

Computer Column

MIKE PIFF

Some utilities

The extensibility of Modula-2 enables us to add on any features we desire, provided the compiler gives us access to the operating system. Two generally desirable features are a random number generator and the ability to query whether any key of the keyboard has been pressed. We illustrate these for a PC.

The random number generator is mathematically simple, but provides a minor problem for some compilers. There is the question of precision of reals and cardinals. It is preferable for the generator to work with long arithmetic even if the resulting random real number is only short. Thus, on some compilers the trailing 'L's on constants and LONG/SHORT conversions will be unnecessary. You will have to consult your documentation on this point; if reals and cardinals are both long by default then you have little to worry about. The following illustrates what we might have to do if reals and cardinals are both short by default.

The implementation closes with an initialization of the *seed* variable using a funny function of the system time.

The second utility is much easier to implement. We simply ask the operating system whether the input buffer has a keypress waiting.

```
DEFINITION MODULE Utils;
PROCEDURE KeyPressed():BOOLEAN;
PROCEDURE rand():REAL;
END Utils.


IMPLEMENTATION MODULE Utils;
FROM System IMPORT Trap, AX, CX, DX;
CONST
  high=256;
  checkstatus=high*11;
  dosInt=33;
PROCEDURE KeyPressed():BOOLEAN;
VAR
  dummy:CARDINAL;
BEGIN
  AX:=checkstatus;
  Trap(dosInt);
  dummy:=AX;
  RETURN (dummy MOD high)#0;
END KeyPressed;
CONST
  m=1771875L; a=2416L;
  c=374441L;
  gettime=high*44;
VAR
  seed:LONGCARD;
PROCEDURE rand():REAL;
BEGIN
  seed:=(seed*a+c) MOD m;
  RETURN
    SHORT(FLOAT(seed)/FLOAT(m));
END rand;
BEGIN
  AX:=gettime;
  Trap(dosInt);
  seed:=LONG(DX)+LONG(CX);
END Utils.
```

Find all solutions of the equation

$$x^{\log y} = y^{\log x}.$$

Letters to the Editor

Dear Editor,

Growing plants and Chinese mathematics

I am amused and amazed by the fact that the two letters solving the *Growing plants* problem (Volume 23, Number 1, page 7) give the same time, though different sizes, for different assumptions about what the problem meant. The second solver notes that the common size is an integer. Consequently I have examined these approaches in general and discover that they always give the same time! Further, the second and more correct solution often gives the size as an integer.

Consider one plant, which grows amount a on the first day and then r times as much on each succeeding day. Then the total growth after t days is

$$A(t) = a\frac{r^t-1}{r-1}$$

as given by Jeremy Bygott (Volume 24, Number 2, pages 57–58). A second plant grows b on the first day and $1/r$ as much on each succeeding day. The total growth after t days simplifies to

$$B(t) = b\frac{r^t-1}{(r-1)r^{t-1}}.$$

Equating $A(t)$ and $B(t)$ gives $r^{t-1} = b/a$ and hence $r^t = rb/a$, so $t = \log_r rb/a$. For convenience, it is easier to have $r > 1$, so we consider the reed first in the original problem and our problem has $a = 1$, $r = 2$, $b = 3$ and so $t = \log_2 6$. At this time, both plants have size $A(t)$, which simplifies to $(rb-a)/(r-1)$. When $r = 2$, this is always an integer when a and b are integers! Even when $r \neq 2$, one can easily choose a and b so that the size is integral.

Barry Christian's solution (Volume 24, Number 1, page 23) assumed that the growth of the first plant on each day was r times the *total* previous growth. Thus he gets $A(t) = a(1+r)^{t-1}$. For the second plant he gets $B(t) = b(1+r^{-1})^{t-1}$. Equating these gives us $r^{t-1} = b/a$ again! Unfortunately $(1+r)^{t-1}$ doesn't come out at all simply, so it is not easy to make the size integral.

The text is exactly as given in the ancient Chinese, but they did not notice the integrality of the size because they had no way of dealing with an exponential function. Instead they observed that the sizes went: 3, $\frac{9}{2}$, $\frac{21}{4}$, ... and 1, 3, 7, ..., so equality must have occurred on the third day and they carried out linear interpolation to find the time. This leads to $\frac{9}{2}+\frac{3}{4}t = 3+4t$, where t is measured from the beginning of the third day. This solves to give $t = \frac{6}{13}$, so equality occurs after $2\frac{6}{13}$ days, when both have size $4\frac{11}{13}$. I found the time of equality as done by Bygott, but did not compute the size at that time, so I did not observe that it was integral.

The *Chiu Chang Suan Shu* (or *Jiu Zhang Suan Shu* in Pinyin) is not a person, but a book and it deserves to be better known. It is the oldest substantial Chinese mathematical work, compiled sometime in the first century AD but reflecting work of the previous two or three centuries. The dating of such a work is a very contentious issue. The earliest version of the text is from the year 263 AD. It claims that

the knowledge existed before the burning of the books in 213 BC and was reassembled by workers in about 150 BC and 60 BC, but a modern scholar says internal evidence puts it between 50 BC and 150 AD.

The Chinese title is usually translated as *Nine Chapters on the Mathematical Art*. The book consists of 246 solved problems. There are lots of surveying, area and volume problems. It finds square and cube roots. One problem involves finding a numerical solution to a quadratic equation by a method that has been identified as Horner's method. The Theorem of Pythagoras is assumed and used. It solves simultaneous linear equations by elimination, both determinate and indeterminate. One problem has five equations in six unknowns.

A remarkable feature is that it has the earliest known use of negatives. 'The method of positive and negative states: for subtracting—same signs take away, different signs add together, positive from nothing makes negative, negative from nothing makes positive; for addition—different signs take away, same signs add together, positive and nothing is positive, negative and nothing makes negative.'

It also contains the oldest examples that I have found of the classical overtaking and meeting problems, of which the given problem is among the most complicated. It occurs in Chapter VII as Problem 11.

Unfortunately there is no English version of this book, but there are German and Russian versions.

Yours sincerely,

DAVID SINGMASTER
(Department of Computing and Mathematics,
South Bank Polytechnic, London)

Dear Editor,

Factorizing the differential operator

Oliver Johnson (*Mathematical Spectrum* Volume 24, Number 2) discusses the Euler homogeneous differential equation

$$p_0 x^n \frac{d^n y}{dx^n} + p_1 x^{n-1} \frac{d^{n-1} y}{dx^{n-1}} + \ldots + p_n y = f(x).$$

Using the substitution $x = e^t$ he establishes by induction that, for all positive integral k,

$$x^{k+1} \frac{d^{k+1} y}{dx^{k+1}} = \left(\frac{d}{dt} - k\right)\left(\frac{d}{dt} - (k-1)\right) \ldots \left(\frac{d}{dt} - 1\right) \frac{dy}{dt},$$

thereby reducing the differential equation to one with constant coefficients. In answer to his query of how well known this formula is, I wish to point out that I mention the general formula on page 79 of my book *Ordinary Differential and Difference Equations* (Van Nostrand, 1965). I establish the result for $k = 0$ and $k = 1$ and say that it is an easy matter for the reader to establish the above general result by induction.

Actually, many years later, it struck me that one can in fact discover the substitution $x = e^t$ in the following way. We note that the coefficient of p_{n-1} in the

above differential equation is $x\,dy/dx$, which can be re-cast thus:

$$x\frac{dy}{dx} = \frac{dy}{(1/x)dx} = \frac{dy}{d(\log x)} = \frac{dy}{dt},$$

where $t = \log x$. In my later years at Aston (before retirement), I took to teaching this to engineering students. It seems to be more satisfactory if one can give a reason for making the substitution $x = e^t$ in the first place.

Yours sincerely,
FRANK CHORLTON
(Department of Computer Science
and Applied Mathematics,
Aston University, Birmingham)

Dear Editor,

$$x^3+y^3 = z^2$$

In *Mathematical Spectrum* Volume 21, Number 3, page 98, K. R. S. Sastry provided some solutions to the equation $x^3+y^3 = z^2$ showing the pattern of the solutions.

I should like to give a general solution for the case when $x+y$ is a square, as follows:

$$x = 4N^4-4K^3N, \qquad y = K^4+8N^3K, \qquad z = 8N^6+20N^3K^3-K^6$$

and then

$$x+y = (2N^2+2NK-K^2)^2.$$

To provide solutions, take K as odd: otherwise a common factor is produced. Conditions can be placed on N and K to provide positive solutions, but as it stands solutions to $x^3-y^3 = z^2$ are also produced.

The solution was obtained by factoring x^3+y^3 using roots of unity and considering each factor as a square. I am currently working on the case of $x+y$ being 3 times a square and should be grateful for any further information from readers.

Yours sincerely,
PAUL YOUNG
(79 Gladstone Street,
Beeston, Nottingham)

Dear Editor,

Bath time with a model

The question on bath filling (*Mathematical Spectrum* Volume 24, Number 2, page 47) suggests a simple mathematical model for any bath with known filling and emptying times.

Suppose a bath takes t_1 minutes to fill and t_2 minutes to empty, where $t_1 < t_2$. Let the volume of the bath be V, the rate of filling be v_1 and the rate of emptying be v_2. Then $V = v_1 t_1 = v_2 t_2$. Let T be the time taken to fill the bath when the plug is out. The new rate of filling is $v_1 - v_2$ and $V = (v_1 - v_2)T$. Therefore

$$T = \frac{V}{v_1 - v_2} = \frac{V}{\frac{v}{t_1} - \frac{v}{t_2}}$$

and hence

$$T = \frac{t_1 t_2}{t_2 - t_1}.$$

For the problem with $t_1 = 3$ and $t_2 = 4$, $T = 12$.

The answer is not intuitively obvious and the simple model shows a useful application.

Yours sincerely,
DAVID GRIGG
(Richmond upon Thames College, Twickenham)

Dear Editor,

Three 1's make 32

In Volume 24, Number 1, Alan Fearnehough posed the following question: 'Using three 1's and any of the usual mathematical symbols, make the number 32.' Here are two solutions:

(a) $\left|\left[\frac{1}{\sqrt{.1}} \div (-.1)\right]\right|$, (b) $\left|\left[\frac{\sqrt{.1}}{.1} \div (-.1)\right]\right|$.

Yours sincerely,
GEORGE STEFANIDIS
(117–01 Park Lane South B5N, Kew Gardens, NY 11418, USA)

Problems and Solutions

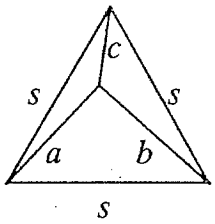
Sixth formers and students are invited to submit solutions to some or all of the problems below: the most attractive solutions will be published in subsequent issues. When writing to the Editorial Office, please state your full name and also the postal address of your school, college or university.

Problems

24.7 (Submitted by Thanh Tuan Tran, a student at the University of California, Berkeley)
What is the maximum number of regions into which a circle can be divided by n straight lines?

24.8 (Submitted by Seung-Jin Bang, Seoul)
Show that the integer $16n^2+8n(-1)^n-3$ is of the form $k(k+4)$ for some integer k.

24.9 (Submitted by Russell Euler, Northwest Missouri State University)
Determine s in terms of a, b and c.



Correction to Problem 24.5 in Volume 24 Number 2
A sentence was omitted in error from this problem. The problem should read:

> There are n students present at a mathematics lecture. Every two students are either friends of each other or strangers to each other. No two friends have a friend in common. Every two strangers have two and only two friends in common. Show that each student has the same number of friends at the lecture.

We apologize to readers who have been puzzling over this and to Gregory Economides, who submitted the problem.

Solutions to Problems in Volume 24 Number 1

24.1 A 'sad' number is a number such that, if its digits are squared and added, and this is repeated, the result is not 1. A 'happy' number is a number which is not sad. All the digits but 5 appear in the first twelve happy numbers; the twelfth happy number is 68.
(i) Verify that all sad numbers iterate to 4.
(ii) Which is the first happy number in which the digit 5 appears?

Solution by Amites Sarkar (Trinity College, Cambridge)

(i) Pick a positive integer n. First we show that we can reduce this number to 130 or less after a suitable number of iterations. Define $N_0 = 10^{10}$ and $N_{m+1} = 10^{N_m/100}$ for $m \geqslant 0$. Then (N_m) is an increasing unbounded sequence, so there is a unique positive integer r such that $N_{r-1} \leqslant n < N_r$, unless $n < 10^{10}$. If $n \geqslant 10^{10}$, there are no more than $N_{r-1}/100$ digits in n (because $n < N_r$), each of which squares to no more than 81, so, after one iteration, we have a number that is no more than $(81/100)N_{r-1}$, so that it is strictly less than N_{r-1}. Therefore we need no more than r iterations to reduce n to a number that has no more than 10 digits.

Denote the operation of squaring digits and adding by α. Then, if $p < 10^{10}$, $\alpha(p) \leqslant 810$, so that

$$\alpha^2(p) = \alpha(\alpha(p)) \leqslant 7^2+9^2+9^2 = 211, \qquad \alpha^3(p) \leqslant 1^2+9^2+9^2 = 163.$$

Either $\alpha^3(p) = 89$, 98 or 99, in which case $\alpha^4(p) = 145$ or 162 and $\alpha^5(p) = 42$ or 41, or $\alpha^3(p) \leqslant 7^2+9^2 = 130$. It is now sufficient to show that all positive integers less than 131 iterate either to 1 or to 4, and this may be verified directly.

(ii) By direct verification, the first happy number containing 5 is 356.

Also solved by Mark Blyth (Gresham's School, Holt).

24.2 Investigate the shape of the face of a rhombic dodecahedron and discover what this has to do with a regular tetrahedron and a sheet of A4 paper. (See the book review in Volume 24, Number 1, pages 30–31.)

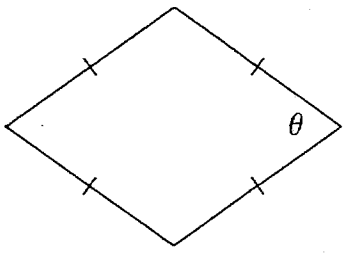
Solution

Consider the cube with the eight vertices $(\pm1, \pm1, \pm1)$. The six midpoints of the faces are $(\pm1, 0, 0)$, $(0, \pm1, 0)$ and $(0, 0, \pm1)$. Consider four bevelled planes meeting at $(1, 0, 0)$:

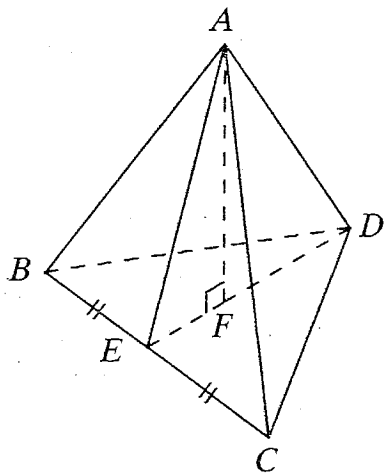
	Plane through	Parallel to	Equation
1	$(0, 1, 0)$	Oz	$x+y = 1$
2	$(0, 0, 1)$	Oy	$x+z = 1$
3	$(0, -1, 0)$	Oz	$x-y = 1$
4	$(0, 0, -1)$	Oy	$x-z = 1$

The intersection of planes 1 and 2 is the line with equation $\boldsymbol{r} = (x, 1-x, 1-x)$ and direction $(1, -1, -1)$. The intersection of planes 1 and 4 is the line with equation $\boldsymbol{r} = (x, 1-x, x-1)$ and direction $(1, -1, 1)$. Let θ be the angle between these directions. Then

$$\cos\theta = \frac{1+1-1}{\sqrt{3}\times\sqrt{3}} = \frac{1}{3}.$$



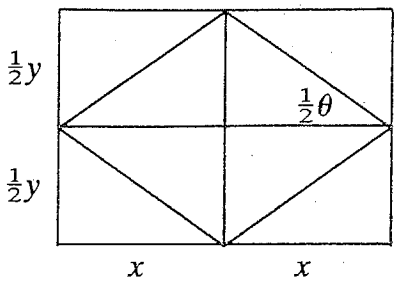
Face of a rhombic dodecahedron



Regular tetrahedron

Consider the regular tetrahedron shown. Since $EF = \frac{1}{3}ED = \frac{1}{3}EA$, $\cos\angle AED = \frac{1}{3}$, so that the angle between the faces is $\cos^{-1}\frac{1}{3}$ and triangle AED (a plane of symmetry) is the shape of half a face of the rhombic dodecahedron.

An A4 sheet can be cut as shown into two A5 sheets, each similar to an A4 sheet. Hence $y/x = 2x/y$ so that $y/x = \sqrt{2}$. Let $t = \tan\frac{1}{2}\theta$, where $\cos\theta = \frac{1}{3}$ as before. Then $(1-t^2)/(1+t^2) = \frac{1}{3}$, giving $t = 1/\sqrt{2}$. This gives the angle shown as $\frac{1}{2}\theta$, so that the shape of a face of a rhombic dodecahedron can be made by joining the midpoints of the edges of a sheet of A4 paper.



A4 sheet

Also solved by Amites Sarkar.

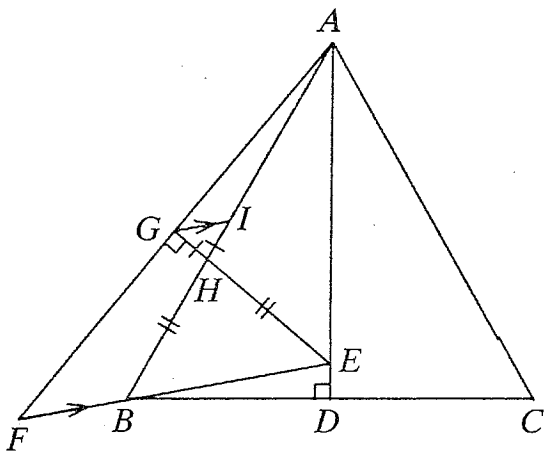
24.3 Determine the exact value of $\cot 80° + \operatorname{cosec} 40°$.

Solution 1 by Matthew Phillips (Richard Hale School, Hertford)

$$\begin{aligned}\cot 80° + \operatorname{cosec} 40° &= \frac{\cos 80°}{\sin 80°} + \frac{1}{\sin 40°} \\ &= \frac{\cos 80° + 2\cos 40°}{\sin 80°} \\ &= \frac{\cos 80° + 2\cos(120° - 80°)}{\sin 80°} \\ &= \frac{\cos 80° + 2\cos 120°\cos 80° + 2\sin 120°\sin 80°}{\sin 80°} \\ &= \frac{2\sin 120°\sin 80°}{\sin 80°} \\ &= \sqrt{3}.\end{aligned}$$

Solution 2 by Amites Sarkar

ABC is an equilateral triangle with $AB = 2$. D is the midpoint of BC. E lies on AD so that angle BED is 80°. F lies on EB produced so that lengths AE and FE are equal. G is the midpoint of AF. EG meets AB at H. I is the midpoint of AB. Write a and b for lengths AE and ED, respectively.



As triangle AEF is isosceles, angles BEH and AEG are both equal to 50°. Angle HBE is also 50°, so that triangle BEH is isosceles. Therefore lengths EH and BH are equal.

Meanwhile triangles AGI and AFB are similar, telling us that GI is parallel to FB. So GI and BE are parallel too, and angles HGI and HIG are both equal to 50°. It follows that triangle GHI is isosceles and that the lengths GH and IH are equal.

Adding, lengths EG and BI are equal. But I bisects AB so EG has length 1. Finally, AEG is a right-angled triangle so we can write

$$\cot 80° + \operatorname{cosec} 40° = b + a = \sqrt{3}.$$

Also solved by Mark Blyth.

Reviews

Wittgenstein's Lectures on the Foundations of Mathematics, Cambridge, 1939. Edited by CORA DIAMOND. The University of Chicago Press, 1990. Pp. 300. £10.25 (ISBN 0-226-90426-1)

As the title indicates, this book is based on lectures given by Ludwig Wittgenstein at Cambridge in 1939. Cora Diamond has, with great care and almost reverence, created this book from the notes of four people who attended the lectures: R. G. Bosanquet, N. Malcolm, R. Rhees and Y. Smythies. There are 31 lectures in the book. I am afraid I found reading it rather tedious, and the ideas rather repetitive. I suspect these were lectures one should have participated in rather than read about. I cannot say that the book enlightened me as a teacher of mathematics, and I would not look at it again. Perhaps it would sit more happily on the shelves of a philosopher.

United World College of the Atlantic, South Glamorgan PAUL BELCHER

The Enjoyment of Mathematics. By HANS RADEMACHER and OTTO TOEPLITZ. Dover, New York, 1990. Pp. 205. £4.45 (ISBN 0-486-26242-1).

First of all, I must confess that when I picked up this book, I did not expect to like it. Quite apart from the pretentious title, a quick flick through it revealed to me that it was composed of about thirty chapters, each of a few pages, and each treating one separate mini-topic. My immediate apprehension was that it would, like many of its genre, fall into the usual trap of trying to fit far too much mathematical meat into each chapter, without giving the reader sufficient motivation or interest in the problems in hand to hold his attention. Now it cannot be claimed that *The Enjoyment of Mathematics* avoids this fault altogether, but I thought that, on the whole, the balance was very skilfully judged, and that the result was a book that is both immensely readable and mathematically rich.

The problems that the authors deal with cover a wide area. For me—and of course, this judgement will be highly personal—the best chapters of the book were those on Waring's problem, closed self-intersecting curves, and the indispensability of the compass in elementary geometry; really excellent were the authors' exposition of Euler's problem and hence the five-colour theorem (so close ...), and Schwarz's breathtaking proof that the pedal triangle has the smallest perimeter of all triangles inscribed in a given triangle. There were, as is almost inevitable in a work of this sort, bad spots too. Most of these seemed to arise when a topic which I felt was not intrinsically that interesting was given a dry and lifeless treatment: one's appreciation of a mathematical problem tends to be increased if one is told why it might be considered important, or how it fits into mathematics in a wider sense. Chapters which I thought were particularly at fault were those on periodic decimal fractions, and 'Some Combinatorial Problems'—the latter being a rather lengthy and tortuous journey through various special cases of finding how many ways there are of putting a collection of coloured balls into jugs. However, there are enough sections in the book for a few poor ones to be quite forgivable; there is

certainly enough well-presented material to keep anyone likely to be reading this review happy for many hours.

A couple of minor warnings may be in order. The first arises from the fact that the text of the book has not been altered since it was first published in English in 1957 (although this edition is new); the four-colour problem, for example, is cited as unsolved. The second warning is perhaps more serious: ignore all the publisher's blurb on the back cover about it 'requiring no more mathematical background than plane geometry and elementary algebra'; this is not particularly accurate, and anyone who can cope with the density of mathematical argument in parts of this book is likely to have more than enough background knowledge anyway. These quibbles aside, I am glad to say that my initial trepidation was quite unfounded, and I would not hesitate to recommend this book to anyone who does not mind mixing mathematical business with a good deal of pleasure.

Trinity College, Cambridge AMITES SARKAR

Discrete Algorithmic Mathematics. By STEPHEN B. MAURER AND ANTHONY RALSTON. Addison-Wesley Publishing Company, Wokingham, 1991. Pp. xix+889. £42.75 (ISBN 0-201-15585-0).

'Our book has both a central object—algorithms—and two central methods—the inductive and recursive paradigms.' Thus the authors, in their preface, encapsulate the theme of this book.

The prologue gives an application which presages both the subject matter and the point of view of the rest of the book. Chapter 0 introduces standard concepts, notations and operations used throughout the book (e.g. the function concept, set notation, matrix multiplication) and Chapter 1 discusses algorithmic language, key issues in the analysis of algorithms and complexity ideas. Chapter 2 is an excellent presentation of mathematical induction as the foremost method of solution and proof in discrete mathematics. In Chapter 3 various graph- and tree-searching paradigms are introduced and used to determine the shortest paths, connectivity, two-colourability and minimum spanning trees. Chapter 4 provides a traditional development of fundamental counting methods up through inclusion–exclusion. Chapter 5 is devoted to difference equations (used synonymously with 'recurrence relations') as a fundamental tool on a par with differential equations. Chapter 6 focuses on discrete probability and Chapter 7 on propositional calculus, including natural deduction, Boolean algebra and the verification of algorithm correctness. Chapter 8 is devoted to algorithmic linear algebra. The theory is developed out of algorithms; Gaussian elimination, eigenvalues and Markov chains pervade the chapter. Chapter 9 provides a bridge between discrete and continuous mathematics. There are sections on series, order notation, generating functions, finite differences and approximation algorithms. In the epilogue, the authors summarise through a detailed study of sorting many of the themes introduced hitherto and provide a bridge to more advanced courses on discrete mathematics.

The book includes 77 section problem sets, 11 supplementary problem sets and a challenging final problem set which leads the reader into several other applications. The sets are large and varied, both in gradation of difficulty and in topics covered. Hints and answers are provided to about half the problems.

This is a monumental volume that contains a phenomenal amount of information, touching on all discrete topics of notable use in many disciplines, not just in mathematics and computer science; it has taken the authors ten years to write! It is on the expensive side, but any shelf of discrete mathematics books is bare without it.

Medical School, University of Newcastle upon Tyne GREGORY D. ECONOMIDES

On the Shoulders of Giants: New Approaches to Numeracy. Edited by LYNN ARTHUR STEEN. National Academy Press, Washington, DC, 1990; distributed by Wiley, Chichester. Pp. vi+232. Hardback £15.55 (ISBN 0-309-04234-8).

On the Shoulders of Giants presents a vision of the richness of mathematics expressed in essays on change, dimension, quantity, shape and uncertainty. Change encourages us to throw away the textbooks that move ploddingly from arithmetic to algebra to calculus. Dimension emphasises the need to provide hands-on experience with higher-dimensional geometry throughout the school years. Quantity examines how to apply mathematical knowledge to such diverse matters as census data, inflation trends and computer security. Shape explores how to create a greater consciousness of shape in the learning process. Uncertainty describes how we can understand the workings of data and chance. The essays in this volume are intended as a vehicle to stimulate creative approaches to mathematics curricula in the next century. The volume itself is part of a US national dialogue on mathematics education. It will be of value to those who develop mathematics curricula, to students training to teach and to practising teachers of mathematics.

Medical School, University of Newcastle upon Tyne GREGORY D. ECONOMIDES

One Hundred Problems in Elementary Mathematics. By HUGO STEINHAUS. Dover, New York, 1990. Pp. 174. £3.70 (ISBN 0-468-23875-X).

The word 'elementary' in the title should not be interpreted as 'easy'. Although only mathematics up to, but not including, calculus is required to solve the problems, their solutions do require clear logical thinking, insight and imagination. The hundred problems are put together in categories in six chapters. Fully worked and often elegant solutions are given, taking up 120 pages of the book. There is also one chapter of 13 problems with no solutions given. The author states that the majority of these have not as yet been solved, but beguilingly does not indicate which ones these are. Martin Gardner, in the foreword, praises the book, saying that the problems are top-drawer and that most of them are relatively new and not found elsewhere. It is a very enjoyable book to dip into and then to ponder over the problems. It is also excellent value for money. Many of the problems are suitable for talented sixth-form students and would be very good practice for students who have progressed to the later rounds of the National Maths Contest, for example.

United World College of the Atlantic, South Glamorgan PAUL BELCHER

The New Ambidextrous Universe. By MARTIN GARDNER. W. H. Freeman, Oxford, 1990. Pp. 392. 112 Illustrations. Hardback £15.95 (ISBN 0-7167-2092-2).

Once again Martin Gardner has produced an excellent book, the readable and entertaining though informative style of which will be familiar to many. In this work he has chosen as his theme the topic of symmetry and asymmetry, which leads the reader out of the realm of mathematics and into the very forefront of recent physical research. Indeed, two revisions have been necessary since the original publication in 1964, owing to 'unbelievable' new discoveries, the nature of which shall be withheld.

The opening chapters assume the light and humorous vein adopted by Gardner in his many 'mathematical puzzle' books, as he reveals many tricks and curiosities involving mirrors. The reader's interest having thus been caught, one is taken on a thorough and systematic examination of various manifestations of symmetry in crystals, molecules and living matter. Some of the detail may seem a little tiresome to the reader hungry for explanation and theory, and indeed much of it is peripheral to the central matter. However, one soon emerges in the world of theoretical physics, which will probably be of more interest to the mathematical reader. Having managed to tie symmetry in with many diverse topics, the author concludes with a very precise account of the theory of superstrings—as far as is conceivably possible from the original question of mirrors.

The cover note promises to answer such vexing questions as: Could the Universe have a twin? If the sundial had been invented in the Southern hemisphere, would clocks move anticlockwise? Would time move backwards? Whilst these questions are more complicated than they might at first appear, the reader of this marvellously informative book will be as well placed to answer them as any non-specialist.

Sixth form, Gresham's School, Holt N. P. SALTMARSH

The Art of Probability for Scientists and Engineers. By RICHARD W. HAMMING. Addison-Wesley, Redwood City, CA, 1990; Pp. xvii+344. £40.45 (ISBN 0-201-51058-8).

Words such as 'for scientists and engineers' in a book title often imply a less than rigorous mathematical approach. This is certainly not the case here. This is a probability book that can be read and valued by mathematicians, and I would have been happy for them to have been included in the title. The author's explanations and reasoning are clear and make enjoyable reading. He uses tables of values and diagrams well to illuminate what is happening. He also includes tables of experimental data that he has simulated by computer to compare with his theoretical results. The author's engineering background means that he adds a new perspective on some of the problems—for example, what he calls 'robustness'—exploring what happens if there are small changes in the original probabilities. I intend to try some of his methods for solving problems on some investigations I have been working on, and I thank him for re-igniting my interest. He applies his methods to problems that one can relate to, and I especially liked it when he successively applied his different methods to the same problem. I gained considerably from reading his book; my only reservation would be its price.

United World College of the Atlantic, South Glamorgan PAUL BELCHER

CONTENTS

ISSN 0025-5653

PRICES (*postage included*)

Prices for Volume 24 (Issues Nos. 1, 2, 3 and 4)

Subscribers in	*Price per volume*	
North, Central and South America	US$13.00 or £7.00	(Note: These overseas prices apply even if the order is placed by an agent in Britain.)
Australia	$A17.00 or £7.00	
Britain, Europe and all other countries	£6.00	

A discount of 10% will be allowed on all orders for five or more copies of Volume 24 sent to the same address.

Details of reduced prices for two- and three-year subscriptions available on request.

Back issues

All back issues except Volume 1 are available; information concerning prices and a list of the articles published may be obtained from the Editor.

Enquiries about rates, subscriptions and advertisements should be directed to:

Editor—Mathematical Spectrum,
Hicks Building,
The University,
Sheffield S3 7RH, UK

Published by the Applied Probability Trust

Typeset by The Pi-squared Press, Nottingham, UK

Printed by Galliard (Printers) Ltd, Great Yarmouth, UK