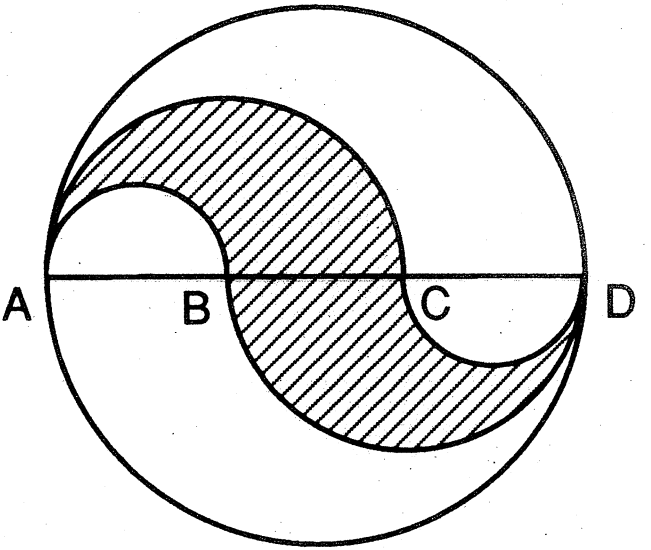
Function

Founder Editor G. B. Preston

Volume 17 Part 2

April 1993



A SCHOOL MATHEMATICS MAGAZINE

Aust. Post Publ. No. VBH0171

FUNCTION is a mathematics magazine addressed principally to students in the upper forms of secondary schools.

It is a 'special interest' journal for those who are interested in mathematics. Windsurfers, chess-players and gardeners all have magazines that cater to their interests. FUNCTION is a counterpart of these.

Coverage is wide — pure mathematics, statistics, computer science and applications of mathematics are all included. Recent issues have carried articles on advances in mathematics, news items on mathematics and its applications, special interest matters, such as computer chess, problems and solutions, discussions, cover diagrams, even cartoons.

* * * * *

Articles, correspondence, problems (with or without solutions) and other material for publication are invited. Address them to:

The Editors,
FUNCTION,
Department of Mathematics,
Monash University,
Clayton, Victoria, 3168.

Alternatively correspondence may be addressed individually to any of the editors at the mathematics departments of the institutions listed on the inside front cover.

FUNCTION is published five times a year, appearing in February, April, June, August, October. Price for five issues (including postage): $17.00*; single issues $4.00. Payments should be sent to the Business Manager at the above address: cheques and money orders should be made payable to Monash University. Enquiries about advertising should be directed to the business manager.

*$8.50 for *bona fide* secondary or tertiary students.

* * * * *

FUNCTION

Volume 17 *Part 2*

(Founder editor: G.B. Preston)

CONTENTS

THE FRONT COVER

Figure 1, below, should be familiar to most readers. A circle with diameter *ABC* is divided up in the following way.

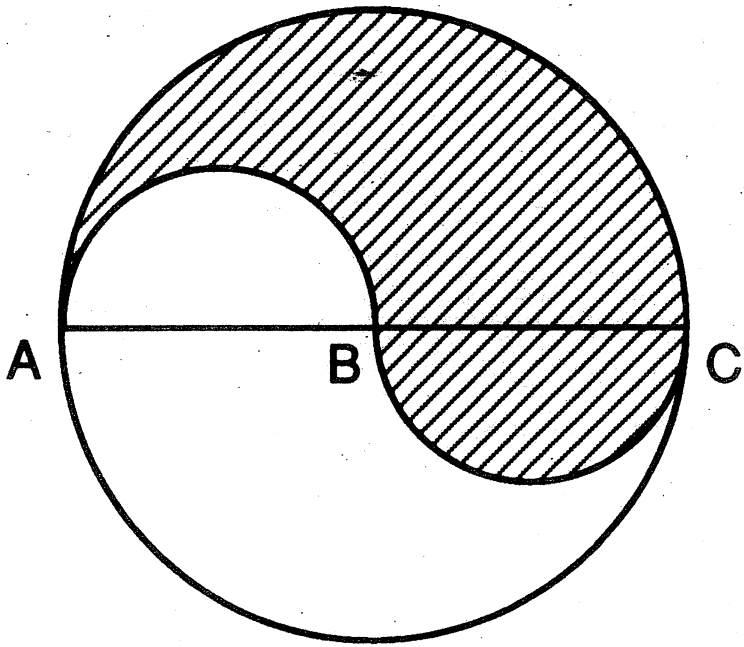


Figure 1

Let *B* be the mid-point of the diameter *ABC* (in fact, the centre of the circle), and construct semi-circles on the new diameters *AB*, *BC*, exactly as shown. The original circle is thus divided into two regions, which by symmetry are equal.

By a rather pleasing aesthetic, however, each is seen to jut into the other's "territory" and so to represent the interplay of two complementary principles. These have been identified in a "new age" reinterpretation of traditional Chinese philosophy as Yin (female) and Yang (male).

The mystic elements of this identification we leave to others. The geometry is relatively trivial. But how many readers know of our cover diagram – an extension in which the diameter of the original circle is trisected, rather than bisected?

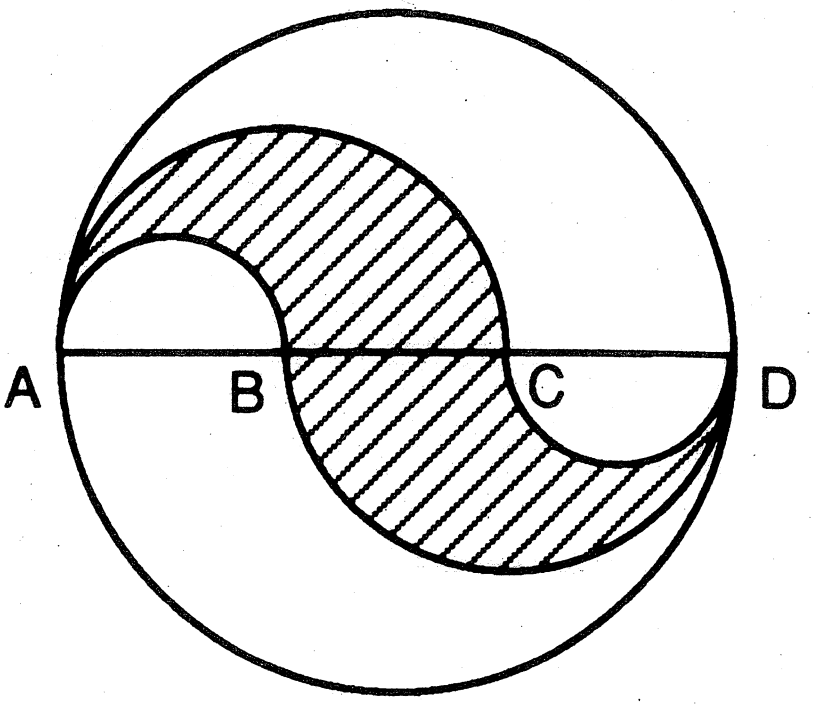


Figure 2

Figure 2 reproduces our cover diagram and the rather surprising fact is that each of the three different regions occupies 1/3 of the total area of the original circle.

This, not difficult, but certainly not widely known, result is to be found in Durell and Wright's *Elementary Trigonometry* (London: 1927).

And now suppose we cut the original diameter into 4, 5, ... parts. What happens then?

THE HARMONIC SERIES†

Peter Grossman, Monash University

From Harmony, from heavenly Harmony
This universal frame began."
J. Dryden

The musings of scholars in ancient Greece, a mysterious number that's probably irrational (but no-one really knows), a problem about cards in packets of breakfast cereal, and a way to infuriate your local librarian: all these share a link with an intriguing mathematical object known as the harmonic series. Although we will be taking a look at the harmonic series in a recreational spirit here, the results presented in this article are important in many applications of mathematics to problems in science and engineering.

It was probably the Pythagorean philosophers of ancient Greece who first took an interest in the sequence of numbers 1, 1/2, 1/3. 1/4, 1/5, ... They noticed a close connection between these numbers and the musical notes produced by a vibrating string. A string divided in the ratio given by a number in the sequence would sound a pleasing "harmonic" of its fundamental note when plucked. The Pythagoreans believed that all of nature had an inherent harmony which could be described by such numerical patterns, and this is probably the reason that the name "harmonic sequence" came to be applied to these numbers.

For the rest of this article, our interest will be focused not on the sequence itself, but on two related objects. These are another sequence $\{S_n\}$, where

$$S_n = 1 + 1/2 + 1/3 + 1/4 + \ldots + 1/n$$

and the infinite series known as the *harmonic series*:

$$S = 1 + 1/2 + 1/3 + 1/4 + \ldots .$$

The first problem that comes to mind is this: as n increases, does S_n become as large as we please, or does it approach some finite value? In mathematical terminology, does the series S diverge or converge? Just looking at the series, it's not particularly obvious what it does. Maybe it increases without limit, like the series $1 + 1 + 1 + 1 + \ldots$. On the other hand, the terms keep getting smaller, like the terms in the series $1 + 1/2 + 1/4 + 1/8 + \ldots$. By adding together a few terms of this last series, you can easily convince yourself that it doesn't become arbitrarily large, but approaches a value of 2. (Some readers will recognise this as a geometric series, and will know that it does indeed converge to 2.)

If we try adding a few terms of S together, we get the following results (rounded to 3 decimal places):

---

† This article is a revised version of one that first appeared in *Feedback*, No. 2 (Nov. 1988), pp. 11-12. *Feedback* was an approximate counterpart of *Function*, published briefly by the (then) Chisholm Institute of Technology. For a related article, see Norah Smith's "Infinite Series", *Function*, *Vol.* 1, *Part* 4.

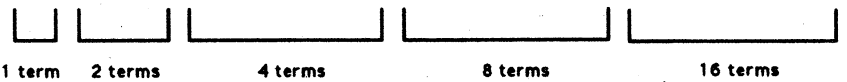
n	1	2	3	4	5	6	7
S_n	1.000	1.500	1.833	2.083	2.283	2.450	2.593

n	8	8	10	20	50	100
S_n	2.718	2.829	2.929	3.598	4.499	5.187

It's not hard to write a program for a computer or a programmable calculator to work out S_n for many more values of n. Even then, it's still not clear just what the series is doing.

To see what is really going on, we need to look at a slightly different series:

$S' = 1 + 1/2 + 1/4 + 1/4 + 1/8 + 1/8 + 1/8 + 1/8 + 1/16 + 1/16 + \ldots + 1/16 + 1/32 + 1/32 + \ldots + 1/32 + \ldots$



Some of the terms in S' are equal to the corresponding terms in S. For instance, the first, second and fourth terms of both series are 1, 1/2 and 1/4 respectively. Other terms have been made smaller: 1/3 has been reduced to 1/4, for example, while 1/5, 1/6 and 1/7 have all been reduced to 1/8. By adding the grouped terms in S', we see that S' is equal to $1 + 1/2 + 1/2 + 1/2 + 1/2 + 1/2 + \ldots$. We now see that S' increases without limit as we add more and more terms; and, since the terms of S are even larger than the terms of S', it follows that S must diverge also.

The harmonic series can be depicted on a graph (Figure 1).

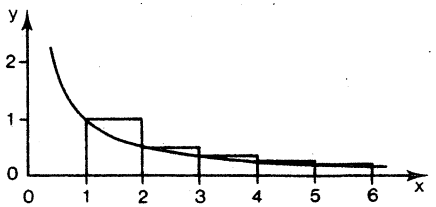


Figure 1

The areas of the bars, from left to right, are 1, 1/2, 1/3, 1/4, ..., so S_n is the total area of the bars up to the bar from n to $n+1$ on the x-axis. The curve shown in the graph is the hyperbola $y = 1/x$, so we see that S_n is slightly larger than the area under the curve between $x = 1$ and $x = n+1$. (If you have met the natural logarithm function in your studies, you will know that this area is $ln\ (n+1)$. This provides another proof that the harmonic series diverges, since $ln\ (n+1)$ increases without limit as n increases.) The difference between the harmonic series and the area under the curve is represented by the parts of the rectangles that extend above the curve. Their combined area is a number called Euler's constant, and it equals about 0.5772. Although it was first investigated more than two centuries ago, no-one yet knows whether Euler's constant is rational or irrational.

The finite harmonic series S_n makes an appearance in the following problem in probability theory. Suppose that a manufacturer of breakfast cereal produces a set of six different cards, and includes one card in every cereal packet. You are keen to have a complete set of cards, so you keep buying packets of cereal until you have at least one of each of the six cards.. Of course, you would have to buy at least six packets, but it is very likely you would need to buy more. On average, how many packets would you expect to have to buy? The answer turns out to be $6(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6})$, or 14.7. Thus you would expect to have to buy about 14 or 15 packets. In general, if there are n different cards, you would need to buy nS_n packets, on average, in order to obtain at least one of each of the cards.

Finally, here is an application of the harmonic series to a problem in mechanics. If we place a book on a table so that part of the book projects over the edge, it won't fall if we allow at most half the length of the book to overhang. Suppose now that we place two identical books, one on top of the other, with the top one overhanging the second by half its length, and the second book overhanging the edge of the table. In order to remain stable, it can be shown that the lower book can overhang by at most one-quarter of its length. With three books, the top one overhangs the second by half its length, the second overhangs the third by one-quarter its length, and the third overhangs the table by one-sixth its length. You an probably guess what happens as we continue to add books. The situation is shown in Figure 2.

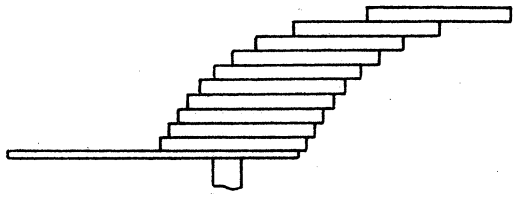


Figure 2

With the ten books shown, the front of the top book overhangs the edge of the table by $\frac{1}{2} S_{10} \simeq 1.464$ book-lengths.† Since the harmonic series diverges, we can make the top book overhang as far as we like, if we have enough books! A stack from table-top to ceiling, containing (say) 100 books, would overhang at the top by an alarming $\frac{1}{2} S_{100} \simeq 2.594$ book-lengths. You could try this next time you are in the library. Who said mathematics wasn't fun?

† In computing such sums, it is best to heed the advice given in the Computer section of *Function*, *Vol.* 16, *Part* 5 and start at the end, rather than at the beginning.

A CLASSIFICATION OF CUBIC POLYNOMIALS

J.B. Henry, Deakin University

The relationship between the graph of the parabola and its equation $y = ax^2 + bx + c$ is well-known. The effects of changing a, b and c and the position of the graph, the number of roots and the discriminant $b^2 - 4ac$ are studied in most senior secondary school courses. Less well-known are similar properties for the cubic $y = ax^3 + bx^2 + cx + k$.

First, there are a number of different shapes for graphs of this general kind. We can reduce the number of curves to be considered by noting certain properties of scale and reflection:

1. We need only consider the case where the coefficient of x^3 is 1: replacing x by $x'/(\sqrt[3]{a})$ will only affect the scale if a is positive and also reflect the curve in the x axis if a is negative.

2. Replacing x by $x' - \frac{b}{3}$ will make the coefficient of x^2 zero. This transformation moves the graph to the left or right but does not change its shape.

3. Adding $-k$ to the right-hand side simply raises or lowers the graph without changing its shape.

Thus we need only consider $y = x^3 + cx$ as the equation to the general cubic curve for the purposes of classifying shapes of curves.

In particular we will investigate the number and position of stationary points for this graph. At stationary points, the derivative $\frac{dy}{dx} = 3x^2 + c$ is zero. Solution of this quadratic gives $x = \frac{\pm\sqrt{(-12c)}}{6} = \frac{\pm\sqrt{(-3c)}}{3}$. Thus the cubic equation can have zero, one or two stationary points according as $3c$ is positive, zero or negative.

If $c = 0$, the equation for the cubic is $y = x^3$. The one stationary point is a point of inflection. See Figure 1 overleaf.

If $c < 0$, the graph has two turning points. These occur when $x = \frac{\pm\sqrt{(-3c)}}{3}$.

Constructing a sign diagram for $\frac{dy}{dx}$ shows that the turning points are a maximum (on the left) and a minimum (on the right). E.g. for $c = 3$, $y = x^3 - 3x$ and the graph is as shown in Figure 2 overleaf.

Notice other features of Figure 2: for large negative values of x, y will be large and negative, for large positive values of x, y will be large and positive. So the graph goes from third quadrant to first quadrant via two turning points – if these are not points of inflection, the maximum must come to the left of the minimum.

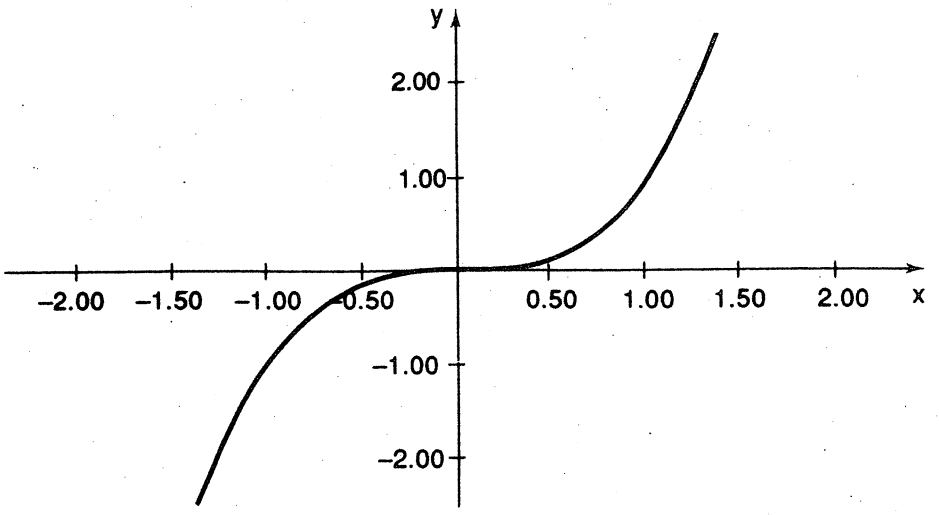


Figure 1

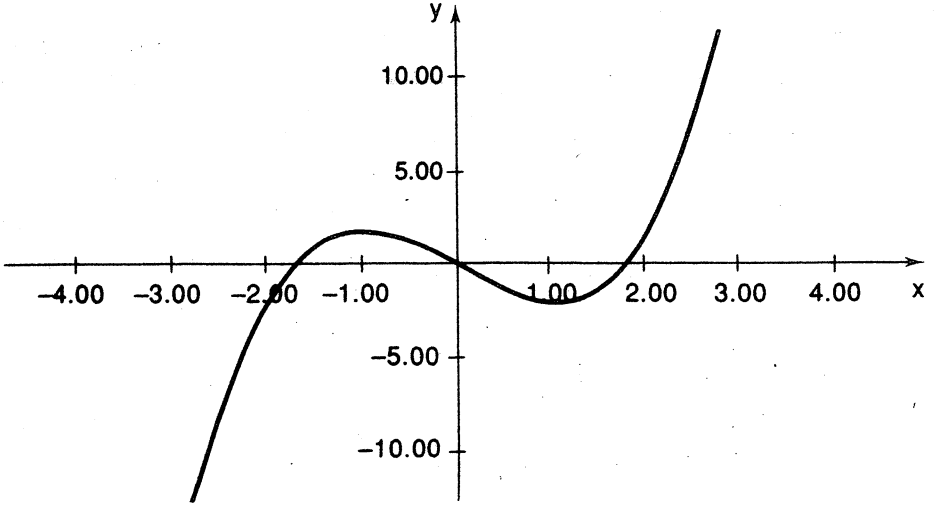


Figure 2.

Now we investigate the case in which there are no stationary points, i.e. when $c > 0$. Figure 3 shows the graph of $y = x^3 + 3x$.

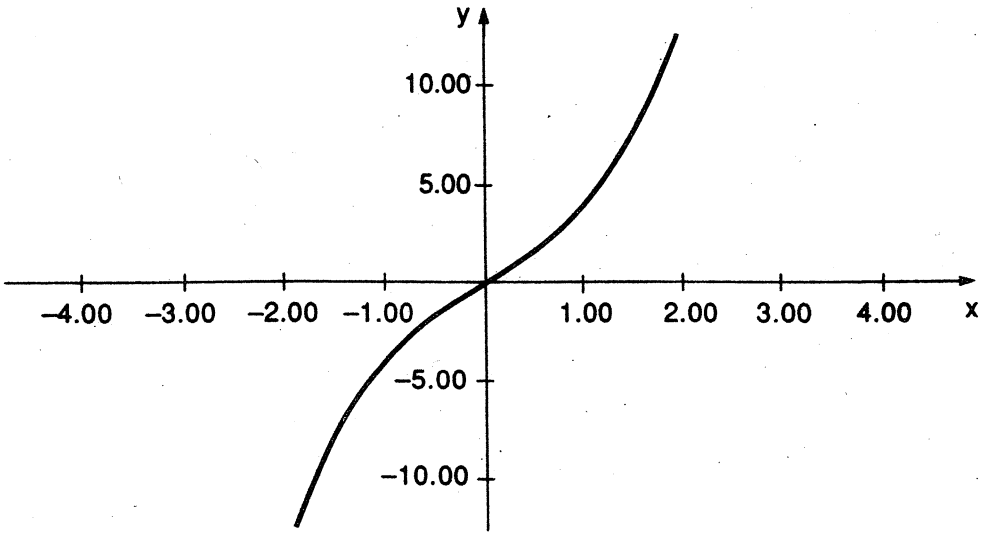


Figure 3

Notice that the gradient is always positive, so a minimum gradient exists.†

This minimum gradient occurs when the derivative

$$\frac{dy}{dx} = 3x^2 + 3$$

is minimised. Of course, the graph of the derivative lies entirely above the x-axis, and the minimum point of the graph is readily found to be (0, 3). The curve $y = x^3 + 3x$ is "concave down" for $x < 0$ and "concave up" for $x > 0$. The direction of "flexure" changes at $x = 0$, which is therefore described as a "point of inflection" (but not a stationary point of inflection, such as we saw in Figure 1).

† Of a set of numbers, all greater than zero, at least one positive minimum must exist. This is a theorem, but should be obvious on careful thought.

In the general case, if $c > 0$ and $y = x^3 + cx$, then $\frac{dy}{dx} = 3x^2 + c$. The minimum value of $\frac{dy}{dx}$ is c and it occurs when $x = 0$. Thus c is always the least value of the gradient.

Thus we see that cubic graphs can be classified into three types:

1. Curves with two stationary points – one maximum, one minimum,
2. Curves with one stationary point – a point of inflection,
3. Curves with no stationary points, just a non-stationary point of inflection.

In order to demonstrate how we can determine to which type a particular curve belongs, we consider an example.

Let $y = x^3 + 3x^2 - 4x + 7$. Then put $x = x' - 1$.

So $y = (x' - 1)^3 + 3(x' - 1)^2 - 4(x' - 1) + 7$

$= (x')^3 - 3(x')^2 + 3x' - 1 + 3(x')^2 - 6x' + 3 + 4 + 7$

$= (x')^3 - 7x' + 13.$

We ignore the constant and consider only $y = (x')^3 - 7x'$. As $-7 < 0$, the curve has two stationary points.

To find these points, set the derivative equal to zero, i.e.

$$3(x')^2 = 7,$$

so

$$x' = \pm\sqrt{\tfrac{7}{3}}.$$

In the original notation therefore

$$x = 1 \pm \sqrt{\tfrac{7}{3}}.$$

The negative sign gives a maximum and the positive a minimum.

Further exploration of the situation is left to the reader.†

* * * * *

† The considerations given here have been generalised to higher polynomials and to other functions including functions depending on two or more variables. If, in the present case, we take the minimum value of y as a point of interest, the corresponding value of x satisfies the equation $3x^2 + c = 0$ and the minimum exists if and only if $c < 0$. More complicated conditions obtain in the higher cases and much recent study has been devoted to them. This branch of Mathematics is called "Catastrophe Theory" and it was discussed in *Function*, *Vol.* 1, *Part* 2. [*Eds.*]

TRIPLE BILL

Michael A.B. Deakin, Monash University

Near where I live is a billboard. This is hardly remarkable, you might think. But this billboard is a little different. For about 5 seconds it shows an ad for facial tissues. At the end of this period, there is a delay of a second or so while the facial tissues are replaced by an ad for a brand of whisky. This in its turn is on display for 5 seconds or so till it too takes a second to disappear and be replaced by a third ad – for a line of menswear. When this too has had its turn, we wait a further second and the facial tissues come back. The cycle continues with the three ads sharing the space, and the attention of the passers-by.

It isn't difficult to see how the board works. There are a number of equilateral triangular prisms all lined up. Face No. 1 of each carries a strip of the facial tissue ad, Face No. 2 a strip of the whisky ad and Face No. 3 the menswear.

But there is some quite interesting mathematics involved, though none of it is very difficult if we approach it from the right aspect.

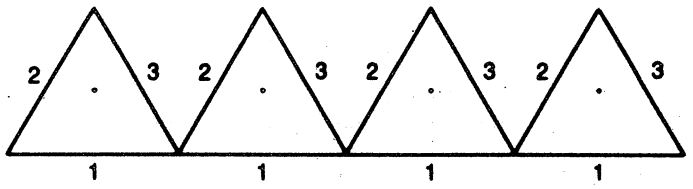


Figure 1.

Figure 1 shows a horizontal cross-section of part of the billboard. Each prism has an equilateral triangular cross-section and each is pivoted at its "centre". The front of the billboard corresponds in the diagram to the base of the triangles in Figure 1, and clearly if the triangles rotate (anticlockwise, say), each left-hand side becomes the base and so we form the second ad, and so on.

Now if we had square instead of equilateral triangular prisms, four displays would be possible, but the motion taking one display to the next would not. The square prisms would all be jammed together (Figure 2).

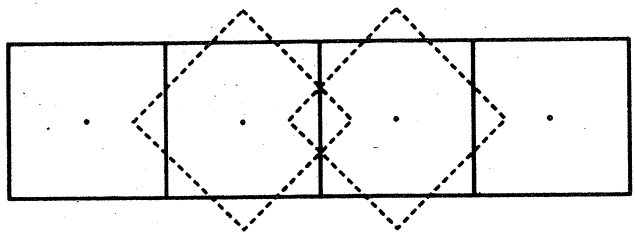


Figure 2.

This is because the "diameter" of a square – its greatest width – is its diagonal, which is longer than its side. Thus, as indicated in Figure 2, the squares could not rotate without overlapping, which is impossible in real life. Similar remarks apply to rectangles (which we'll come back to) and also to pentagons, hexagons and the like. (Anything with five or more sides would not line up nicely anyhow.)

But let's now look in more detail at the motion of the triangles.

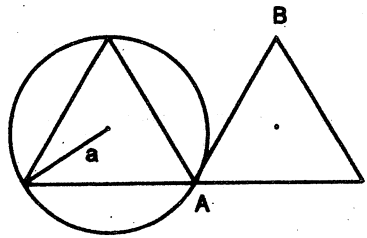


Figure 3.

The "diameter" of the triangle is equal to its side and the triangle may be inscribed in a circle centred on the centroid of the triangle. This circle is swept out by each vertex of the triangle as it rotates. If the radius of the circle is a, the side of the triangle is $a\sqrt{3}$ and the distance from the centre (the shortest, perpendicular, distance that is) to a side is $\frac{1}{2}a$. (Can you prove these statements?)

Now if in Figure 3 the right-hand triangle were fixed in the position shown, the left-hand triangle could still rotate. The side AB will not interfere with the motion as it is tangent to the circle. [Again, can you prove this?] This can be important because sometimes the mechanism that turns one of the triangles breaks down and one strip of (say) the whisky ad stays in place all the time, looking a little out of place among the tissues or the menswear, but not throwing the whole billboard out of action.

But now suppose that the right-hand triangle stopped in some other position. See Figure 4.

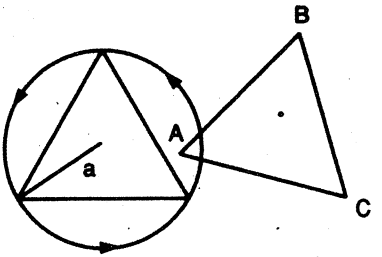


Figure 4.

Now the vertex A lies very much in the way of the left-hand triangle and if it encounters that triangle it will be pushed out of the way. In fact, from the position diagrammed, the right-hand triangle would be pushed all the way until the side CA was tangent to the circle. At this point it would once again be out of the way of the left-hand triangle and also of the next (undrawn) triangle to the right of triangle ABC. When this happens, the point C will face forward (down in the diagram) [again the proof is left to the reader], and so pieces of two ads will remain on view until a repair is carried out.

Now that we've looked at what can go *wrong*, let's now turn our attention to the correct functioning of the billboard. In normal functioning, the two triangles turn at the same speed, so we have Figure 5.

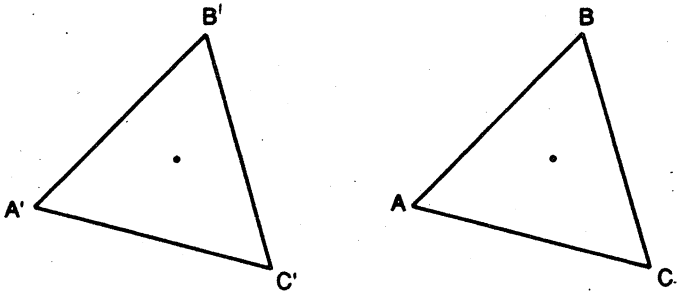


Figure 5.

$A'B'$ and AB remain parallel and I have drawn the triangles as indeed they should be without any overlap. Can we be sure such overlap cannot occur?

We can, and here is one way to see it. The mid-point, D, of the side AB moves on a circle of radius $a/2$. [This circle is the *envelope* of the various positions of the side AB; see *Function*, *Vol.* 5, *Part* 1.] AB is always tangent to this circle. [Again you should prove this yourself.]

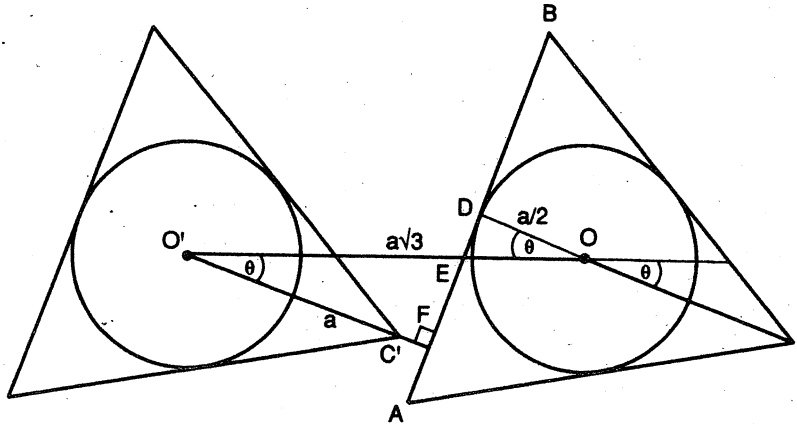


Figure 6.

Look now at Figure 6. O', O are the centres of the two circles, and the distance from O' to O is $a\sqrt{3}$. Let the line $O'O$ meet the line AB at E. Further, let EO make an angle θ with $O'O$. $O'C$ will then also make an angle θ with $O'O$.

Now we readily see that $EO = \frac{a}{2\cos\theta}$. Thus $O'E = a\sqrt{3} - \frac{a}{2\cos\theta}$. Thus the perpendicular distance from O' to AB ($O'F$ call it) is

$$(a\sqrt{3} - \frac{a}{2\cos\theta})\cos\theta.$$

Thus $C'F = (a\sqrt{3} - \frac{a}{2\cos\theta})\cos\theta - a$

$$= a\sqrt{3}\cos\theta - \frac{3a}{2}.$$

We need to assure ourselves that this distance is always greater than or equal to zero. Clearly it will be zero while an ad is on display, i.e. when C' coincides with A. At such a time, $\theta = 30°$. When $\theta = -30°$ we are halfway through the transition and C' will coincide with B (at the back of the billboard).

So we need to show that $a\sqrt{3}\cos\theta - \frac{3a}{2} > 0$ if $-30° < \theta < 30°$. This is so and I leave it to you to prove it.

Some questions remain. Could we use the coincidence of C with B (at the back) to create a 2-sided billboard? The answer is "no" – for two reasons. Can you find them?

We could, however, have a double billboard alternating two ads, though quadruple ones, quintuple ones, etc. are out, as we have seen. The panels would have to be very thin – rectangles won't rotate, again as we saw earlier. This would lead to problems with the drive mechanism – but there are ways by which this could be overcome. Presumably triple billboards attract three sponsors and are thus more profitable than double ones, that allow only two. So if we are to construct a moving billboard, it might as well be a triple one.

HISTORY OF MATHEMATICS SECTION

EDITOR: M.A.B. DEAKIN

Over most parts of the earth, there are pronounced seasonal changes, and the pattern of daily life, the work that needs to be done, must conform to these naturally imposed rhythms. This sets up an annual cycle and it becomes important to any reasonably complex society to keep accurate account of this.

The best-known example is that of the ancient Egyptians, whose agriculture depended upon an annual Nile flood, the arrival of which had to be predicted so that fields could be readied for it. But all societies need such accounting of days – Lapps must be able to know when to migrate with their herds of reindeer and we ourselves need to know when to buy winter woolies or new summer gear.

The cycle of the seasons is, as we now know, the result of the earth's revolution around the sun, while the much faster alternation of day and night is due to the rotation of the earth about its own axis. There are approximately 365 days in a year. That is to say that, after about 365 day-night cycles, the earth will have returned to the same point of space that it occupied beforehand. We shall see, however, that this is not an adequate approximation.

But first, look at how we might keep track of the passage of the year. Because the sun goes around the earth and the earth has an axis inclined at about $23\frac{1}{2}^\circ$ to the plane of the earth's orbit, the sun appears to us to move north and south in the sky as the year progresses. For us in Australia, the sun is to our north for most of the year and over most of the continent. On December the 22nd, our longest day, it appears to come just far enough south to be overhead at noon at Rockhampton and Alice Springs – and to be slightly to the south for points north of these, say Cairns and Darwin.

This yearly motion of the sun provides one way to construct a calendar, and it is now widely accepted that Stonehenge, the famous megalithic monument in southern Britain, was actually an astronomical observatory for use in this connection.

Other cultures used different techniques. It was probably the ancient Persians who first marked the passage of the year by noting which constellation replaced the sun on the horizon at dusk and gave way to it each morning. The twelve such constellations remain familiar to us as the names given to the signs of the zodiac, and faint echoes of ancient Persian thought probably still remain in some of the various competing systems of astrology.

Yet other calendars have been constructed from the phases of the moon. Over long (very long) periods of time, we observe, on average, 12.368267 full moons per year. This rather complicated number makes lunar calendars rather difficult to use in practice. Attempts to combine lunar and solar cycles result in the *very* complicated "lunisolar" calendars. This method of constructing a calendar began with the Babylonians and survives in Jewish and Islamic religious practice.†

† And also in the determination of the date of the Christian Easter (see *Function, Vol. 9, Part 3*). This will form the subject of a later column.

In fact, many different calendars have been constructed, but for the rest of this article, the focus will be on our own calendar, its structure and its antecedents.

There are, in fact, 365.242199 days in a year – a figure now established by very precise astronomical observation. It is accommodated by making some years to be of 365 and others of 366 days, according to various formulae and rules. But first note that if we simply approximated this number by the nearest integer, 365, we would run, reasonably soon, into trouble.

Each year a discrepancy of 0.242199 days would occur and these discrepancies would accumulate. An 80-year old would find that the summer solstice (longest day) came almost three weeks later in the year than it had in his early childhood, and even bigger discrepancies would build up over several generations. This is a feature that will recur in our story.

Our present calendar has its early origin in that of ancient Rome – this seems to have been a rather clumsy and complicated affair, with a considerable *ad hoc* element (i.e. "fudge factor") to it. Some details are given, insofar as they have been reconstructed, in the *Encyclopedia Britannica* article on the calendar. Interested readers are referred to this source.

We pick up the story in the middle of the 1st century B.C., when Julius Caesar sought the help of an astronomer called Sosigenes in setting up a better system. Sosigenes abandoned the attempt to use the moon, and he also adopted the value $365\frac{1}{4}$, in place of 365, as the number of days in a year. By 46 B.C., discrepancies that had crept in under the previous system had accumulated and so Caesar introduced extra days into that year, making it 445 days long. The new system began in the following year. Important minor details have changed in the days since 45 B.C., but the Julian Calendar (as it came to be called – after Julius Caesar) remained in force until very modern times. (In fact it is still used, though in a modified form, for ecclesiastical purposes in the Orthodox Christian churches.)

As that calendar became settled, and there were European countries even that didn't abandon it till this century, it comprised twelve months: the familiar January, February, ..., December. These months have their origins in the old lunisolar calendars – indeed, the word "month" has the same root as the word "moon", but the moon now plays no part in their determination. This was the first of Sosigenes' reforms. Because 12 is the closest integer approximation to 12.368267 (the exact number of lunar months in a year), there are 12 months with an average of 30.4375 days in each.

It might perhaps have been arranged a little more neatly, but what eventuated was that eleven months acquired fixed lengths: 4 at 30 days and 7 at 31. The twelfth month, February, was given 28 days if the year (Y) was not a multiple of 4 and 29 if it was.[†] This ensured an average year-length of 365.25 days – the second of Sosigenes' reforms.

[†] It will be recalled that the zodiacal calendar also had 12 "months": Aries (22 March-22 April), ..., Pisces (22 Feb.-22 March). It would of course be a phenomenal coincidence if the sun actually moved from one "house" to the next in accordance with the lengths of our conventional months. Indeed, this doesn't happen. Some astrologers, I'm told, take cognisance of this fact. Most do not.

When I was at school, we were taught a rhyme that gave the lengths of the Julian months.

Thirty days hath September
April, June and November;
All the rest have thirty-one
Save for February alone.
That has twenty-eight days clear,
But twenty-nine in each leap year.
In each leap year, one in four,
February gets one day more.

The Julian calendar was a clear advance on all preceding ones and for civil purposes, as opposed to religious or ecclesiastical ones, it took over more or less world-wide. Greece retained it till 1924, Turkey till 1927 and China did not finally abandon it till 1929.

However, over long periods of time, the Julian calendar is still not sufficiently accurate. The year is actually 365.242199 days long, and Sosigenes had approximated this figure to 365.25. The discrepancy is 0.007801 days per year. This doesn't seem very much, but over 1000 years, it comes to over a week: 7.801 days in fact. By the year 1500, the discrepancy would have been 11.7015 days had counting begun in the year 0. Actually it didn't, but by 1545 the (Northern Hemisphere) spring equinox (used to set the date of Easter) was 10 days out.

Pope Paul III was, in consequence of this, authorised by the Council of Trent to seek a solution, but it was in fact a later pope (Gregory XIII) who actually made the reform. In 1572 he appointed the Jesuit astronomer and mathematician Christopher Clavius (1537-1612 – see *Function, Vol.* 10, *Part* 5) to produce a system better than the Julian. Clavius was in truth a rather minor figure, but he did have influence with the powerful men of his day.

The reform that he proposed was, in essence, a popularisation of an idea attributed variously to earlier workers. Clavius' biographer in the *Dictionary of Scientific Biography* (H.L.L. Busard) credits the idea to Erasmus Reinhold (1511-1553), but Reinhold's biographer in the same work makes no reference to calendric studies. Reinhold's biographer (Owen Gingerich) places his subject second only to Copernicus in the list of leading 16th Century mathematical astronomers. [Both Clavius and Reinhold opposed the Copernican theory, although the former remained a firm friend of Galileo – even while working for Cardinal Bellarmine, usually seen as one of Galileo's main opponents.]

The *Astronomical Ephemeris*† instead attributes Clavius' ideas to suggestions by the astronomer-physician Luigi Lilio (or Aloysius Lilius), who died in 1576. Little seems to be known about Lilio. A German reference work, *Poggendorf's Wörterbuch*, notes his connection with the Gregorian calendar and the date of his death, but little else.

Either way, Clavius' report found favour with the pope and the new calendar (called the Gregorian, after Pope Gregory) was promulgated in February 1582.

The simplest way to describe Clavius' reform is to say that he replaced Sosigenes' figure of 365.25 by 365.2425. For this is in fact the outcome. The Gregorian calendar makes a small departure from the Julian in the way that leap years are determined.

† See the references at the end of this article.

Let Y be the year. If Y is not divisible (exactly) by 4, then Y is not a leap year. However, if $Y/4$ is integral, it will be a leap year except that:

If $Y/100$ is integral, but $Y/400$ is not, then Y is not a leap year.

So, immediately after Pope Gregory's announcement, 1584 was a leap year, as both the old and new calendars would have had it, and so were 1588, 1592, 1596 and indeed 1600. The first difference occurred in the year 1700. On the Julian calendar, 1700 was a leap year, but on the Gregorian it was not (although divisible by 4, 1700 is also divisible by 100, but not by 400). The years 1800, 1900 were Julian, but not Gregorian, leap years. (I recall my grandmother telling me that 1900 was not a leap year – much to her surprise.) The year 2000, however, *is* to be a leap year as 2000 is exactly divisible by 400. 2100, 2200 and 2300 will not be leap years; 2400 will be. And so it will go on.

There is little, very little, difference between the two calendars – 3 days, to be precise, since Pope Gregory issued his edict. However, what Pope Gregory also did was to make the new calendar retrospective. To overcome the 10-day discrepancy in the date of the equinox, he decreed that the day after October the 4th, 1582 was to be October the 15th. So ten days simply ceased to exist.

This ruling, or something similar to it, was rapidly accepted and adopted in Catholic countries like Austria and Spain. Protestant countries, however, saw little reason to take any notice of an edict by the pope of Rome, nor did Orthodox countries like Russia or non-Christian countries like Japan.

Almost 350 years were to elapse before scientific common sense overcame religious bigotry and the Gregorian calendar prevailed. Britain finally went Gregorian in September 1752, deleting the eleven days (10 plus the discrepancy caused by the year 1700) 3-13 (inclusive) of that month. This occasioned riots to the cry "Give us back our 11 days!" Some history books present this as a demonstration of public ignorance and stupidity, but the rioters had a point: landlords were permitted by law to charge rent for the 11 non-existent days, and most did.

The other point to note is that dates of important historical events may vary – depending on which calendar the narrator is using. So on December the 21st 1605, the Spanish explorer de Quiros set out to find Australia, and he was presumably using the Gregorian calendar. On January the 4th 1688, the English privateer Dampier landed in Western Australia – my source (*Macquarie*) does not make it clear if this is a Julian or a Gregorian date. The question is particularly vexed for this period in Australian history, as so many of the early landfalls were made by the Dutch. Catholic states of the Netherlands went Gregorian in 1582/1583. The Protestant states waited till 1700/1701. Whether Tasman, for example, used a Julian or Gregorian calendar for his log-book is unclear to me. Sometimes also modern historians correct original Julian dates to Gregorian for the benefit of contemporary readers, sometimes not.

Clavius' approximation, 365.2425, exceeds the true value, 365.242199 by 0.00301 days per year. Over a 400-year cycle, this amounts to 2.8896 hours. Thus, it may be that, after some dozen or so such 400-year cycles, we may need to remove another day from the calendar. None of us need worry unduly about this – we may safely leave it to our very remote descendants.

Finally, notice another nice feature of Clavius' calendar. We not only break the year into months, a vestige of the earlier luni-solar calendars, but we also divide it into even shorter periods called weeks. The week has no astronomical significance whatsoever and is merely a device for the social ordering of civic life. (Which makes it

quite extraordinary that it is almost universally agreed.) It probably derives from the attempt to break the lunar month (29.530589 days) into smaller periods – although greater accuracy could have been achieved by taking three 10-day weeks to the month.

The seven-day week, however, is celebrated in the book of Genesis, which shows that it is very old. It underlies the worship of all the great monotheistic religions, which differ (in this respect) only in which day is considered holy (Muslims: Friday; Jews: Saturday; Christians: Sunday). Moreover, it has been almost universally adopted, even well outside this context.

However, neither 365 nor 366 is divisible by 7. This means that there is never an exact integral number of weeks in a year. An ordinary year has 52 weeks and one extra day; in a leap year there are two extra days.

The effect of this is that, as 1993 began on a Friday, 1994 will begin on a Saturday. Similarly 1995 will begin on a Sunday and 1996 on a Monday. However, 1996 is a leap year and so 1997 will begin, not on a Tuesday, but on a Wednesday, and so on. The leap years (normally) come around every four years and there are seven days in the week. So, because the numbers 4 and 7 are relatively prime, the calendar usually cycles through a 28-year period.

My parents, now in their 80s, have a collection of calendars from earlier days. Hanging on their wall this year is a recycled 1965 calendar. It is the same as that for 1993. In fact, a collection of 14 different calendars will cover any conceivable year: for the year may begin on Sunday, Monday, ..., Saturday, and may either be or not be a leap year. No further variation is possible.

Were we to use the Julian method of reckoning, the 28-year cycle would continue forever. Under the Gregorian regime, however, this steady cycle will be interrupted in 2100.

Astronomers classify years according to their "Dominical letter". The word (from the Latin "dominus" = lord, and referring to the "Lord's day") and the method by which it is assigned show clearly the ecclesiastical influence on our calendar. 1993 began on a Friday and the first Sunday ("Lord's day") was January the 3rd. So 1993 is assigned the Dominical letter C, C being the third letter of the alphabet. 1992 had a Dominical letter D and 1994 will be classified as B. When we come to leap years, the pattern changes a little. 1996 begins as G, because it begins on a Monday and its first Sunday is Day 7 (i.e. January the 7th). However, once March the 1st arrives, the pattern has altered, because of the intervention of February the 29th. The rest of the year the calendar is the same as that for a year beginning on a Tuesday (i.e. an F-type year). So 1996 is classified as GF.

We have the following table.

Year	Type	Year	Type	Year	Type	Year	Type
1980	FE	1987	D	1994	B	2001	G
1981	D	1988	CB	1995	A	2002	F
1982	C	1989	A	1996	GF	2003	E
1983	B	1990	G	1997	E	2004	DC
1984	AG	1991	F	1998	D	2005	B
1985	F	1992	ED	1999	C	2006	A
1986	E	1993	C	2000	BA	2007	G
						2008	FE

And so the cycle continues. (Notice how the 14 types of year distribute themselves over the 28-year period.)

However, as already noted, when 2100 comes along, the pattern will be disrupted. How badly, let us ask. Well, badly enough, but not so *very* badly.

For Clavius set up a 400-year cycle with what would, under the Julian system, have been 100 leap years, but which, under the new, Gregorian, system that he recommended to the pope, had instead only 97 leap years. So: in the 400-year cycle of the Gregorian calendar, there are 303 ordinary years and 97 leap years. The total number of days is

$$303 \times 365 + 97 \times 366 = 146\ 097$$

and 146 097 is, as it turns out, an exact multiple of 7.

So the pattern by which old calendars may be recycled – the 14 different types – recycles *exactly* every 400 years.

References

The only good and readily available reference is the *Encyclopedia Britannica* article (in the *Macropedia*, under the heading "Calendar"). This indeed deplores the lack of good material in English. It gives, as authoritative but outdated, a work I was not able to consult before writing this article, but also recommends the *Explanatory Supplement to the Astronomical Ephemeris Tables*. (The *Astronomical Ephemeris* replaced the old *Nautical Almanac*.) This source also gives references, most of them hard to come by. A good popular text, not referred to by any of the above, is Margaret Bowman's *Romance in Arithmetic* (published by the University of London). Details on Clavius, Reinhold and Sosigenes are available in the *Dictionary of Scientific Biography*. For related articles in *Function*, see *Vol.* 1, *Part* 1 and *Vol.* 11, *Part* 1.

* * * * *

COMPUTERS AND COMPUTING

EDITOR: CRISTINA VARSAVSKY

A Security Matter†

Which of us has not tried as a child to send encoded messages to be understood only by the receiver who had the key to decode it? How many times were we involved in the deciphering of a mysterious message? We certainly explored many techniques; perhaps the most common one was the substitution of one letter by another. For example, replacing A by C, B by D, C by E, D by F, and so on, the message HAVE A NICE DAY becomes JCXG C PKEG FCA. Anyone who discovers or knows the rule is able to get the original HAVE A NICE DAY back. To make things a little bit more complicated, we may have had a sequence of numbers, say 321, which will code the message by substituting the first letter by the letter three places further in the alphabet, the second by two places, and the third by the following letter, repeating the pattern until the message is finally coded. Using this technique, our message HAVE A NICE DAY will be transformed to KCWH C OLEF GCZ.

† For a related article, see *Function*, *Vol.* 4, *Part* 5.

We can think of all sorts of combinations for substituting letters of shuffling them around. In all these techniques, both parties, the encoder and the decoder, have to know or break the key to transmit and receive the message. Therefore both have the potentiality to code and to decode. This results in a great threat to security when the technique is used in large organizations like banks, where many people have to possess the key to read and send messages (transactions). If the key is leaked by one of these key holders, the security collapses.

In 1976, the researchers Diffie and Hellman at Stanford, and Merkle at the University of California, came up, independently, with a clever encoding system where the secret keys for encoding and decoding were different. Furthermore, while the decoding key was securely locked away, the encoding key could be published. This was a major breakthrough.

Let us see how this works. We start with two prime numbers, p and q, and form their product n. Now we use the Greek letter φ to represent the number of positive integers less than n and relatively prime to n, that is, with non-common non-trivial divisors. Since this φ depends on n it is more appropriate to write it as $\varphi(n)$. For example, $\varphi(4) = 2$ (1 and 3 are relatively prime to 4) and $\varphi(7) = 6$ (1,2,3,4,5,6 have no common divisors with 7). This function $\varphi(n)$ plays an important rôle here and in number theory in general. Since in our case we know the prime factors of n, i.e. $p + q$, there is an easy way to compute $\varphi(n)$: just subtract 1 from each of the primes and multiply the results together, that is

$$\varphi(n) = (p-1)(q-1) \quad \text{because} \quad n = p \times q.$$

(Check for $\varphi(6)$: $6 = 3 \times 2$, then $\varphi(6) = (3-1)(2-1) = 2$ as before.)

Leonard Euler (1707-1783) proved the very important result that any number relatively prime to n, raised to the power of $\varphi(n)$ and then counted in groups of n, will leave a remainder of 1. [So in the case of $n = 4$, $\varphi(n) = 2$, we have, for example,

$$3^2 = 9 = 2 \times 4 + 1$$
$$5^2 = 25 = 6 \times 4 + 1$$
$$27^2 = 729 = 182 \times 4 + 1.]$$

If we use the notation introduced in the last number of *Function* (under the title *Clock Arithmetic*), Euler's result can be written as

$$a^{\varphi(n)} \equiv 1 \pmod{n} \quad \text{if } a \text{ and } n \text{ are relatively prime.}$$

Now let us go back to our problem of encoding and see what the rôles are of p, q, n and $\varphi(n)$ in it. The next step is to find two integers, d (for decoding) and e (for encoding), whose product will give a remainder of 1 when counted in groups of $\varphi(n)$, that is

$$d \times e \equiv 1 \pmod{\varphi(n)}.$$

The integers e and n are made public, while p, q and d are kept secret. Before encoding the message we need to express it as an integer M in some predetermined way, like for example, by assigning

$$\text{blank} = 10,\ A = 11,\ B = 12,\ C = 13,\ D = 14,\ \ldots,\ Z = 36$$

so that HAVE A NICE DAY becomes $M = 1811321510111024191315101141135$. M should be less than both p and q. This is not a problem, because if the message is too long, it may be broken into blocks of smaller messages.

Once we have the message M in a numerical form and the public keys e and n, we proceed with the encoding as follows:

$$E \equiv M^e \pmod{n}.$$

In plain language, E is the remainder of M^e when it is divided by n.

Although this appears to be a complicated calculation if M is large, there are efficient algorithms for doing it quickly.

This number E is sent out and can only be decoded with the secret keys d and $\varphi(n)$ as follows:

$$M = E^d \pmod{n} \tag{1}$$

You may be asking why, but the reason is simple: you only need to observe that

$$\begin{aligned} E^d &\equiv (M^e)^d && \pmod{n} \\ &\equiv M^{ed} && \pmod{n} \\ &\equiv M^{\text{multiple of } \varphi(n)+1} && \pmod{n} \\ &\equiv 1 \times M && \pmod{n} \quad \text{(using Euler's result)} \\ &\equiv M && \pmod{n}. \end{aligned}$$

Thus E^d is congruent to M (mod n), and since we took the precaution of making M less than n, then certainly Equality (1) holds.

Let us see this working through an example, say HAVE A NICE DAY or, in number form, 1811321510111024191315101141135. We first need to choose the two primes p and q. For simplicity we use small primes; in a real situation much larger primes are required. Take, for example,

$$p = 47 \quad \text{and} \quad q = 59.$$

Then

$$n = 47 \times 59 = 2773 \quad \text{and} \quad \varphi(n) = 46 \times 58 = 2668.$$

Now find e and d such that $e \times d \equiv 1 \pmod{2668}$. $e = 17$ and $d = 157$ would do because

$$17 \times 157 = 2669 = 1 \times 2668 + 1 \equiv 1 \pmod{2668}.$$

So we publish $n = 2773$ and $e = 17$, and keep the rest locked away. Since n is not very large, we impose the restriction that we will send one letter of the message (two digits) at a time. In practice, longer blocks are sent at a time as a larger n is used. If the sender wants to send the first letter H, its number form $M = 18$ becomes encoded as

$$E = M^e \equiv 18^{17} \pmod{2773}.$$

We have to be careful when using a calculator to evaluate large numbers like 18^{17}, with more digits than the calculator can handle (22 in this case). Since we only need the remainder when counted in groups of 2773, we can keep the numbers small if we observe that

$$18^{17} = 18^{2^4+1} = (((18^2)^2)^2)^2 \times 18.$$

So we square 18, take only the remainder after counting in groups of 2773, square three more times using arithmetic modulo 2773 and finally multiply by 18. This procedure will keep the numbers less than $2773^2 = 7689529$ which a reasonable calculator can do nicely. Here is the evaluation of 18^{17} in the 2773 arithmetic:

$18^2 = 324 \equiv 324 \pmod{2773}$

$324^2 = 104976 = 37 \times 2773 + 2375 \equiv 2375 \pmod{2773}$

$2375^2 = 5640625 = 2034 \times 2773 + 343 \equiv 343 \pmod{2773}$

$343^2 = 117649 = 42 \times 2773 + 1183 \equiv 1183 \pmod{2773}$

$1183 \times 18 = 21294 = 7 \times 2773 + 1883 \equiv 1883 \pmod{2773}$.

Then $E = 1883$ is the encoded form for $M = 18$, and could be decoded only by the holder of d and n, who simply raises it to the power of $d = 157$ using arithmetic modulo 2773, that is

$$D = 1883^{157} \pmod{2773}.$$

For the same reason as before, we need to keep the numbers small. Observing that $157 = 1 + 2^2 + 2^3 + 2^4 + 2^7$, we write

$$1883^{157} = 1883 \times 1883^{2^2} \times 1883^{2^3} \times 1883^{2^4} \times 1883^{2^7}$$

$$= 1883 \times (1883^2)^2 \times ((1883^2)^2)^2 \times (((1883^2)^2)^2)^2 \times ((((((1883^2)^2)^2)^2)^2)^2)^2.$$

This involves quite a few calculations, but, believe me, gives back the original 18. (Actually, I got $1883^{157} \equiv 18 \pmod{2773}$ straight from my computer algebra package, which amongst many other helpful features performs calculations using clock arithmetic.)

This procedure must be followed for any letter of the message, or every pair of digits. Since this is a repetitive task, the best idea is to have a program that will do it for us. Here I give the main BASIC routines to make it work:

```
1000 REM Routine for encoding
1010 INPUT "Enter a two digit number"; M
1020 REM Calculate M^(2^4) (mod 2773)
1030 ENC=M
1040 FOR n=1 to 4
1050       ENC=ENC*ENC
1060       MODD=ENC:GOSUB 3000 'Operation in arithmetic modulo 2773'
1070       ENC=MODD
1080 NEXT
1090 REM Multiply by M
1100 ENC=ENC*M : MODD=ENC:GOSUB 3000:ENC=MODD
1110 PRINT "The encoded form of "M" is " ENC
1120 STOP
```

(Keep the following code in a safe place!)

```
2000 REM Routine for decoding
2010 INPUT "Enter the encoded number";ENC
2020 AUX=ENC
2030 FOR n=1 to 7
2040       AUX=AUX*AUX
```

```
2040      AUX=AUX*AUX
2050      MODD=AUX:GOSUB 3000:AUX=MODD
2060      If n=2 AUX1=AUX
2070      If n=3 AUX2=AUX
2080      If n=4 AUX#=AUX
2090 NEXT
2100 REM Multiplication of all the powers
2110 DEC=AUX
2120 DEC=DEC*AUX3:MODD=DEC:GOSUB 3000:DEC=MODD
2130 DEC=DEC*AUX2:MODD=DEC:GOSUB 3000:DEC=MODD
2140 DEC=DEC*AUX1:MODD=DEC:GOSUB 3000:DEC=MODD
2150 DEC=DEC*ENC :MODD=DEC:GOSUB 3000:DEC=MODD
2160 PRINT "The decoded form of " ENC " is " DEC

3000 REM Routine for 2773 arithmetic
3010 IF MODD<2773 THEN RETURN
3020 MODD=MODD-2773:GOTO 3010
```

You may be wondering why this system is secure, given that everyone knows the numbers $n = 2773$ and $e = 17$ for encoding. How would a code-breaker find the decoding key from the published keys 17 and 2773? Well, it is sufficient to find the two factors p and q of 2773, which could be done by trying all the different possible primes. Once these are found, $\varphi(n)$ $(= (p-1)(q-1))$ is known and the decoding key d (such that $d \times 17 \equiv 1 \pmod{\varphi(n)}$) can be determined by trial and error. In other words, the security strongly depends on the possibility of finding factors for n. This is an easy task if n is small enough, but what do you do if the published n is 59111321103579513? Would you have a clue how to find the factors when your calculator cannot even handle such a large number? You may argue that although you cannot do it, this is an easy task for a reasonably powerful computer. The reality is that even for the supercomputers like the Cray series, factorizing a 200 digit number is a very challenging task. Although there are fast algorithms for multiplying large numbers, it may take years to figure out the decoding key from an encoding key of, say, 200 digits, even under an assault by a battery of the world's fastest computers. Pure mathematicians and code-breakers are working very intensively on this problem of factorizing on which security systems rely so heavily.

* * * * *

PROBLEMS AND SOLUTIONS

A large number of previously set problems have so far gone unsolved and we here publish solutions to some of these.

SOLUTION TO PROBLEM 13.3.1

The problem read: Given a circle, centre O, radius R, and a point P outside of it, construct a straight line, passing through P, that meets the circle in points A and B such that $PB = 2PA$.

Solution: Through P draw a tangent PT to the circle and touching the circle at T. Then, by a standard theorem in Euclidean geometry

$$PA \cdot PB = PT^2.$$

Thus if $PB = 2PA$, it follows that

$$2PA^2 = PT^2$$

and so $PA = PT/\sqrt{2}$.

It is possible by Euclidean ruler and compass methods to construct the length $PT/\sqrt{2}$ and so to construct the length PA. With centre P and radius PA draw a circle. If this circle intersects the original circle, choose either point of intersection as A. Join PA and continue it to meet the original circle in B.

Notice that the construction will not work if $|OP| > 3R$ and also notice that this is as it should be.

SOLUTION TO PROBLEM 13.4.1

The problem read: Show that, on a 4×4 chessboard, a knight cannot start at any square and visit once only, in turn, each other square of the board.

Solution: A knight moves by proceeding to the opposite corner of a 3×3 rectangle. The problem thus asks for a proof that if the knight is to travel to all squares of the board, then either

(a) it can't actually do this

or

(b) it must visit some squares at least twice before others are visited at all.

Consult Figure 1. This establishes a convenient notation by which the squares may be numbered. If the knight is to visit all squares in some order, then it will visit Square 1. Start there. From here it may go either to Square 7 or to Square 10. Without loss of generality, choose Square 7. From here, the knight may travel either to Square 7 or to Square 10. Without loss of generality, choose Square 7. From here, the knight may travel either to Square 9, Square 14 or Square 16 (but we don't want it to travel back to Square 1).

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Figure 1

In this way, enumerate all paths and show that (b) above applies.

Alternatively, take the centre of each square as a vertex of a "graph" and join all those vertices corresponding to valid knight-moves. These joins will be the edges of our "graph" in the sense of the mathematical discipline known as *graph theory*. Over the years, *Function* has published a number of articles on graph theory (see, e.g., *Vol.* 8, *Part* 3 and *Vol.* 13, *Part* 1).

In graph theoretical terms, the question becomes that of whether a "hamiltonian path" exists and, using theorems from graph theory, it may readily be shown that there is no such path. For more on this, see Chapter 2 of the book *Mathematical Gems*, by Ross Honsberger. (An excerpt from this chapter appeared by permission in *Function*, *Vol.* 1, *Part* 1.)

SOLUTION TO PROBLEM 13.4.2

The problem read: If you watch a game of snooker on video, using the Fast Forward facility, not only is the action greatly speeded up, but the balls come to rest with astonishing rapidity. Why?

Solution: If a ball, travelling with speed u, comes to rest in a distance s, then it is known that its average deceleration a is given by the formula

$$u^2 = 2as.$$

The Fast Forward control speeds up the action by a factor of about 3, so the apparent value of u is about 3 times what the true value is. The apparent value of u^2 is thus about 9 times the true value. However, s remains unaltered and so the apparent a is 9 (rather than 3) times the true value.

The effect is further exaggerated by the fact that many (most) frames are suppressed and invisible in Fast Forward mode and so we miss, typically, the fine detail of the coming-to-rest.

SOLUTION TO PROBLEM 14.4.1

The problem read: Let a be an arbitrary real number. Determine all real numbers x with the property that

$$|x| + |x - 1| + |x - 2| = a.$$

Solution: Note that we need $a > 0$, and indeed we will find that a must exceed 2. There are four possibilities:

(a) $x > 2$, (b) $1 < x < 2$, (c) $0 < x < 1$, (d) $x < 0$.

Examine each case in turn. E.g. Case (b). In this case

$$|x| + |x - 1| + |x - 2| = x + (x - 1) + (2 - x)$$

and we find $x = a - 1$. Then we require

$$1 < a - 1 < 2, \text{ i.e. } 2 < a < 3.$$

We find by such methods:

If $2 < a < 3$, $x = a - 1$ or $3 - a$ (Cases 2, 3)
If $3 < a < 9$, $x = 1 - \frac{a}{3}$ (Case 4)
If $a > 9$, $x = \frac{a}{3} - 1$ or $1 - \frac{a}{3}$ (Cases 1, 4).

If $x = 0, 1, 2$, the analysis is left to the reader. For $a < 2$, no solutions exist.

These results may also be analysed geometrically by use of a number-line.

SOLUTION TO PROBLEM 14.4.2

The problem read: Determine all real numbers x which satisfy the equation

$$\sqrt{x^2-[x]^2} - [x]^2 = 3 - x,$$

where $[x]$ is the largest integer less than or equal to x.

Solution: We note first that if $x < 0$, $x^2 < [x]^2$ and so the left-hand side does not exist and so no solution is possible. Furthermore, if x is large positive, then although both sides of the equation are negative, the left-hand side has a greater magnitude than the right. We are thus able to rule out all x greater than or equal to 2.

Now suppose $0 \le x < 1$, i.e. $[x] = 0$. The equation then reduces to

$$x = 3 - x, \text{ i.e. } x = 1.5.$$

However, $[1.5] = 1 \neq 0$ and so this is no solution either.

Finally consider $1 \le x < 2$, i.e. $[x] = 1$. We now have

$$\sqrt{x^2-1} - 1 = 3 - x$$

i.e.

$$\sqrt{x^2-1} = 4 - x$$

and from this it follows that

$$8x = 17$$

and so $x = 17/8$. However, $[17/8] = 2 \neq 1$.

Thus no solution is possible.

A later issue, *Vol.* 14, *Part* 3 amended the problem to read $\sqrt{x^2-[x]^2} = 3 - x$. This may be solved as above to give $x = \frac{5}{3}, \frac{13}{6}, 3, \frac{25}{6}$ or $\frac{17}{3}$.

SOLUTION TO PROBLEM 14.1.3

The problem read: Prove that 17 never divides any number of the form $2^{(3^n)} + 1$.

Solution: First try some small values of n, and use modular arithmetic notation as described by Cristina Varsavsky in her recent column in *Function*. We find

$$n = 0 : 2^{(3^0)} + 1 = 2 + 1 = 3 \equiv 3 \pmod{17}$$

$$n = 1 : 2^{(3^1)} + 1 = 2^3 + 1 = 9 \equiv 9 \pmod{17}$$

$$n = 2 : 2^{(3^2)} + 1 = 2^9 + 1 = 513 \equiv 3 \pmod{17}$$

$$n = 3 : 2^{(3^3)} + 1 = 2^{27} + 1 = 134217729 \equiv 9 \pmod{17}.$$

This looks as if we have a pattern:

$$2^{(3^{2n})} + 1 \equiv 3 \pmod{17} \quad \text{and} \quad 2^{(3^{2n+1})} + 1 \equiv 9 \pmod{17}.$$

This is indeed the case and we set out now to prove it. First we will show that

$$2^{(3^{m+2})} + 1 \equiv 2^{(3^m)} + 1 \pmod{17}.$$

This will hold if

$$2^{(3^{m+2})} \equiv 2^{(3^m)} \pmod{17}.$$

But

$$2^{(3^{m+2})} \equiv 2^{3^m \times 9} = (2^{3^m})^9.$$

So put first $m = 0$ to find $2^{(3^0)} = 2$, and $2^9 = 512 \equiv 2 \pmod{17}$. Similarly if $m = 1$, we have $2^{(3^1)} = 8 \equiv 8 \pmod{17}$, and $8^9 = 134217729 \equiv 8 \pmod{17}$.

By results derived by Cristina Varsavsky in the previous issue, this pattern must persist and so the result is established.

SOLUTION TO PROBLEM 14.1.4

This problem was initially misprinted (for the correction see *Vol.* 14, *Part* 3). It asked for the proof of two inequalities – one of which is incorrect as it appeared. The other may be written

$$1 + 2^{-1/3} + 3^{-1/3} + \ldots + n^{-1/3} < \tfrac{3}{2} n^{2/3}.$$

Solution: The expression on the left is represented by the area under the "steps" in Figure 2 (see overleaf). Through the right-hand end of each "step", there passes a curve whose equation is

$$y = x^{-1/3}.$$

The area under this curve is

$$\int_0^n x^{-1/3} dx, \text{ i.e. } 3/2n^{2/3}$$

and as this is clearly a larger area, the inequality is proved.

Similarly we may pass the curve

$$y = (x + 1)^{-1/3}$$

through the left-hand ends of all the steps and the area under this will be

$$\int_0^n (x + 1)^{-1/3} dx = \tfrac{3}{2}\left[(n+1)^{2/3} - 1\right].$$

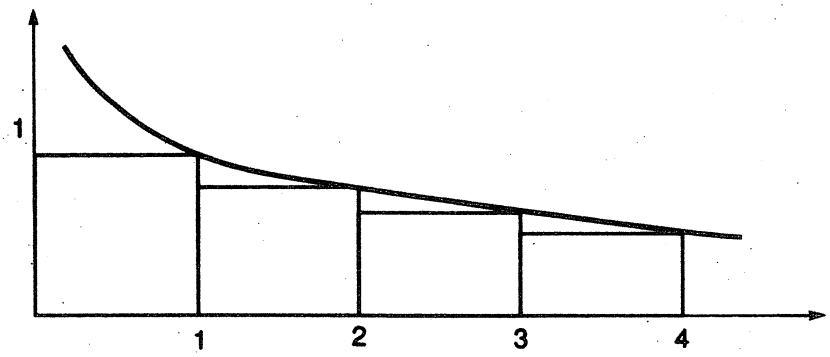


Figure 2

Thus we have

$$\frac{3}{2}\left[(n+1)^{2/3} - 1\right] < 1 + 2^{-1/3} + 3^{-1/2} + \ldots + n^{-1/3} < \frac{3}{2}n^{2/3}$$

and this is how the problem should have read.

The method of argument is similar to that used by Peter Grossman in this issue and indeed the two matters are closely related.

SOLUTION TO PROBLEM 14.2.1

The problem was couched in verse:

They counted some rats in Mayfair
The number was a third of a square
If a quarter were slain
Just a cube would remain
How many at least must be there?

Solution: Expressed more prosaically, we have r rats where $r = n^2/3$. We also are told $3r/4 = m^3$. Thus we seek integers n, m such that $n^2 = 4m^3$. Notice that m^3 must be not only a perfect cube, but also a perfect square. Thus m^3 is a perfect 6th power, Thus set $m^3 = k^6$. Then $m = k^2$ and $n = 2k^3$. So

$$r = \frac{4k^6}{3}$$

and for the number of rats to be integral, k must be a multiple of 3. Put $k = 3l$ and find

$$r = 972k^6.$$

This is one-third of the perfect square 2916 and 4/3 times the perfect cube $729k^6$. The smallest value possible for r is 972, achieved when $k = 1$.

SOLUTION TO PROBLEM 14.2.2

The problem read: Someone was asked how much money he had. He gave as an answer: "I have loaned all my money; to Maevius I gave a third, to Sempronius a fourth of my money, and to Caius I gave 200 thalers, so all my money is gone". How much did the person lend?

Solution: The problem is simple. The answer is 480 thalers.

PROBLEM 14.2.3 concerned the hands of a clock and was answered in essence by Karl Spiteri in his article *Tick Tock* (*Function*, *Vol.* 17, *Part* 1).

SOLUTION TO PROBLEM 14.2.4

The problem read: Someone is fallen upon by robbers. They inquire immediately about his money. Their victim answers: "I have just so much money on me that I can give each of you 5 thalers". They take his money and also his sabre. One of the robbers keeps the sabre and returns 13 thalers to the robbers' community chest whereby now each of the robbers receives 7 thalers. The number of thalers that was the value of the sabre was twice the number of the robbers. Now the question is: how many robbers were there? How much money did the victim carry? And what was the value of the sabre?

Solution: The figures are consistent if there were 10 robbers and the sabre was worth 20 thalers. This answer makes the doubtful assumption that there is honour among thieves!

SOLUTION TO PROBLEM 14.2.5

This problem (also published as PROBLEM 15.5.1) read: In an Australian Rules match, the Galahs beat the Goannas. One fan noticed that the Galahs scored as many goals as the Goannas scored behinds, and *vice versa*. He also noticed that the total points score of the Galahs (read from right to left) equalled that of the Goannas (but read from left to right). What were the scores registered by the teams?

Solution: Each goal is worth 6 points and each behind one point. It is not hard to see that the Galahs scored 10 goals and one behind (61 points) and the Goannas 1 goal and 10 behinds (16 points). It is relatively routine to prove that this is the only possible answer.

PROBLEMS 14.2.6, 14.2.7, 14.2.8 and 14.2.9 all concerned graph theory (see SOLUTION TO PROBLEM 13.4.1 above). PROBLEM 14.2.6 was, apart from details of wording, the same as PROBLEM 3.2.3. A solution was published in *Vol.* 3, *Part* 5. PROBLEM 14.2.7 is trivially easy and PROBLEM 14.2.8 a straightforward consequence of it. PROBLEM 14.2.9 is a specialisation of PROBLEM 14.2.8.

SOLUTION TO PROBLEM 14.2.10

This problem, posed in 1990, asked for the positive integral solutions to the equation

$$x + y + xy = 1990.$$

Solution: First note that if (x, y) is a solution, then so is (y, x). Thus we need consider only those solutions for which $1 \le x < \sqrt{1990}$, i.e. $1 \le x \le 44$. But now x cannot be odd, for if y were odd, then so would $x + y + xy$ be, and this also would hold if y were even. Thus x is even, and so also is y, by symmetry. From here on, although there are doubtless more elegant ways to complete the problem, a simple search (either manually or with computer help) yields a single solution $(10, 180)$.

* * * * *

THE TELECOM 1993 AUSTRALIAN MATHEMATICAL OLYMPIAD

Hans Lausch, Monash University

The Telecom 1993 Australian Mathematical Olympiad was held on the 9th and 10th of February. There were two papers: each of four hours' duration and with no calculators allowed. Here are the questions.

Paper I

1. In triangle ABC, the angle ACB is greater than 90°. Point D is the foot of the perpendicular from C to AB; M is the midpoint of AB; E is the point on AC extended such that $EM = BM$; F is the point of intersection of BC and DE; moreover, $BE = BF$. Prove that angle CBE = 2 angle ABC.

2. For each function f which is defined for all real numbers and satisfies

$$f(x.y) = x.f(y) + f(x).y \tag{1}$$

and

$$f(x + y) = f(x^{1993}) + f(y^{1993}) \tag{2}$$

determine the value $f(\sqrt{5753})$.

3. Determine all triples (a_1, a_2, a_3), $a_1 \ge a_2 \ge a_3$, of positive integers in which each number divides the sum of the other two numbers.

4. For each positive integer n, let

$$f(n) = [2\sqrt{n}] - [\sqrt{n-1} + \sqrt{n+1}].$$

Determine all values n for which $f(n) = 1$.

Note: If x is a real number, then $[x]$ is the largest integer not exceeding x.

Paper II

5. Determine all integers x and y that satisfy

$$(x + 2)^4 - x^4 = y^3.$$

6. In the acute-angled triangle ABC, let D, E, F be the feet of altitudes through A, B, C, respectively, and H the orthocentre. Prove that

$$\frac{AH}{AD} + \frac{BH}{BE} + \frac{CH}{CF} = 2.$$

7. Let n be a positive integer, $a_1, a_2, \ldots, a_n$ positive real numbers and $s = a_1 + a_2 + \ldots + a_n$.

Prove that

$$\sum_{i=1}^{n} \frac{a_i}{s-a_i} \geq \frac{n}{n-1} \quad \text{and} \quad \sum_{i=1}^{n} \frac{s-a_i}{a_i} \geq n(n-1).$$

8. The vertices of triangle ABC in the x-y plane have integer co-ordinates, and its sides do not contain any other points having integer co-ordinates. The interior of ABC contains only one point, G, that has integer co-ordinates. Prove that G is the centroid of ABC.

93 participants sat. Gold certificates were awarded to:

Frank Calegari,	Year 12,	Melbourne Grammar School, Vic.
Nicholas Cavenagh,	Year 12,	St. Thomas More College, Qld.
William Hart,	Year 12,	Elizabeth College, Tas.
William Hawkins,	Year 11,	Canberra Grammar School, ACT.
Anthony Henderson,	Year 12,	Sydney Grammar School, NSW.
Rupert McCallum,	Year 12,	North Sydney Boys' High School, NSW.
Chaitana Rao,	Year 11,	Melbourne Grammar School, Vic.
Simon Schwartz,	Year 11,	Moriah College, NSW.
Anthony Wirth,	Year 11,	Melbourne Grammar School, Vic.

* * * * *

Nice were it Possible

"If the batsman on strike scores a strike-rate of 50% and the batsman at the other end also scores at 50%, then you can expect a score of around 250 [in a 50-over match]."

Richie Benaud, Ch. 9, 20/2/'93

And if the nine batsmen in the pavillion also scored at 50%, what a great score that would be!

Registered for posting as a periodical – "Category B"
ISSN 0313 – 6825

* * * * *

Published by Monash University Mathematics Department