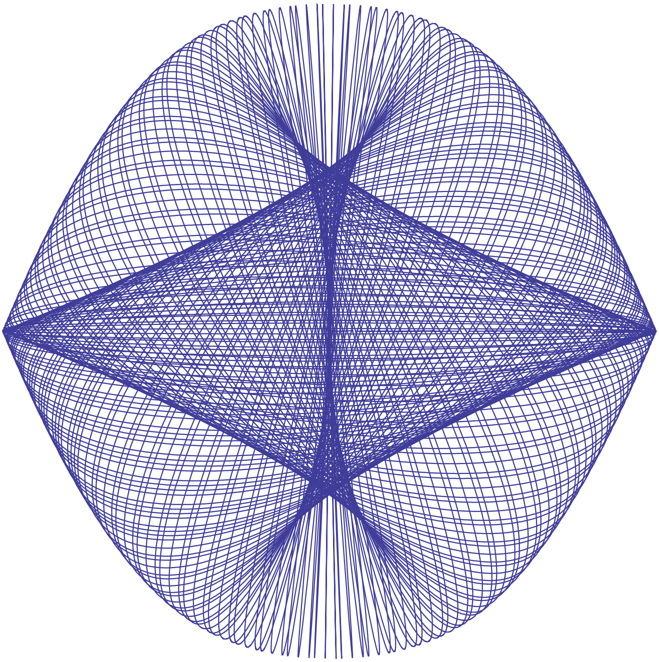
ISSN 1350-8539

# M500 194



# The M500 Society and Officers

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

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

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

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

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

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

# Some maths from long ago

## Envelopes, caustics and the creation of a closed continuous four-cusped curve

### Bob Escolme

Take a piece of waxed paper with a straight line edge (call it $l$) and mark a point $F$ about six centimetres in from $l$, half way down the sheet. Now fold the paper so that any point $P$ on $l$ coincides with $F$ and press the paper so a crease (a thin white line) appears on the waxed surface of the paper. Repeat this process for different points $P$ on $l$ until you tire of the exercise. If you persist, not for all that long, you will find that the creases 'envelop' a curve—a parabola in fact.

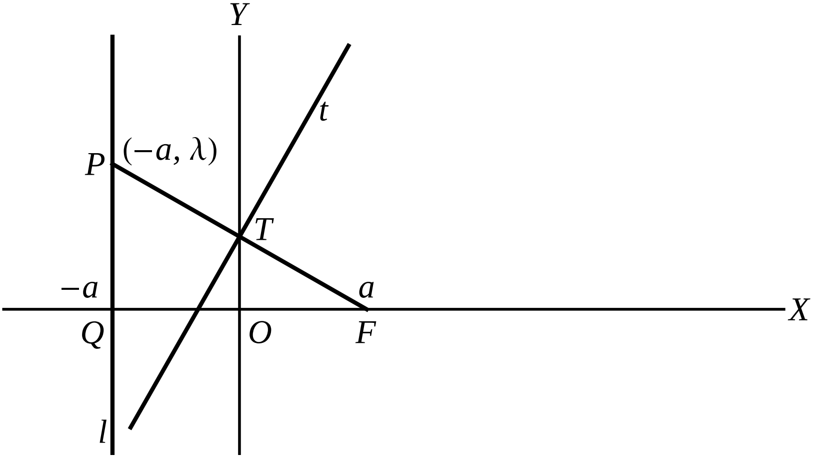
One can say that the dual of a family of points tracing out a curve is a family of tangents enveloping a curve. The theory of envelopes goes a little further—a parametrized family of curves, not necessarily straight lines, form an 'envelope' and one task is to derive the equation of the curve enveloped by the family.

Reverting to the first paragraph, if you take $P$ as a varying point on a circle and $F$ as a point inside the circle, the envelope of the creases will be an ellipse, whereas if $F$ is outside the circle the envelope is a hyperbola. I can still recall the delight I felt when long ago in the VIth form (see later) I did this bit of practical geometry about the conic sections

We can show that the envelope with $P$ varying on a straight line is a parabola as follows. In the figure below, $l$ has equation $x = -a$ and $F$ has coordinates $(a, 0)$. Folding the paper so that $Q$ (coordinates $(-a, 0)$) coincides with $F$, we can see that the $y$-axis is one of the potential creases—i.e. it is one of the family of lines forming our envelope. In general, let $P$ have coordinates $(-a, \lambda)$; then folding the paper so that $P$ coincides with $F$ and creasing the paper in effect creates the perpendicular bisector $t$ of $PF$. The line $PF$ has gradient $-\lambda/2a$ so that $m$, the gradient of $t$, is $2a/\lambda$. Then, using the formula $y = mx + c$ to determine the equation of our crease $t$, and with $T = (0, \lambda/2)$ lying on $t$, we have $\lambda/2 = m \cdot 0 + c \Rightarrow c = \lambda/2$ and so the equation of $t$ is

$$y = \frac{2a}{\lambda}x + \frac{\lambda}{2}, \quad \text{or} \quad 2\lambda y = 4ax + \lambda^2, \tag{1}$$

an equation satisfied by points on the tangents of our envelope for all $\lambda$.



Now, with $P$ at the point $(\lambda+\delta\lambda, 0)$ we get another crease as part of our envelope. Points satisfying (1) and the equation of this second crease also satisfy the difference between the two equations and the equation found by dividing that difference equation by $\delta\lambda$ and going to the limit as $\delta\lambda \to 0$; i.e. the equation found by differentiating equation (1) with respect to $\lambda$, which is

$$\lambda \;=\; y. \tag{2}$$

Thus any point on our envelope satisfies both (1) and (2), which, on eliminating $\lambda$, produces the equation of the envelope: $y^2 = 4ax$.

To establish that the envelope of the creases is an ellipse when the points $P$ lie on a circle, with $F$ inside, is no more difficult in principle, although the algebra is rather more tedious.

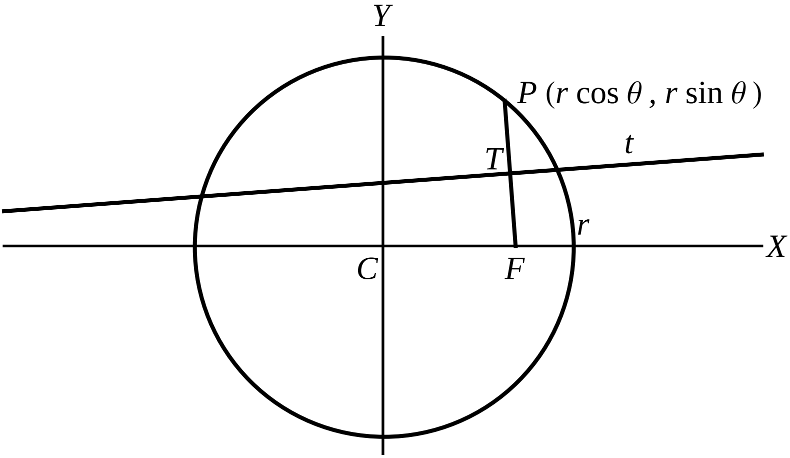
In the figure opposite let $C$, the centre of a circle of radius $r$, be at the origin and $CF$ be part of the $X$-axis. Let $P$ be the point with coordinates $(r\cos\theta, r\sin\theta)$ and $F$ the point with coordinates $(r - 2\alpha r, 0)$ such that $0 < \alpha < 1$ (i.e. $F$ is inside the circle). Then the line $PF$ has gradient

$$m' \;=\; \frac{\sin\theta}{\cos\theta - (1-2\alpha)},$$

which implies that the gradient of our crease $t$, the line through $T$, the midpoint of $PF$, and at right angles to $PF$, is

$$m \;=\; -\,\frac{\cos\theta - (1-2\alpha)}{\sin\theta}.$$

Also, $T$ has coordinates $\left(\frac{r}{2}(\cos\theta + (1-2\alpha)), \frac{r}{2}\sin\theta\right)$.



Substituting these values for the coordinates of $T$ and the gradient $m$ of $t$ in the equation of the straight line $y = mx + c$, we get

$$c \;=\; \frac{r}{2}\sin\theta + \frac{r(\cos\theta - (1-2\alpha))(\cos\theta + (1-2\alpha))}{2\sin\theta},$$

which, thankfully, simplifies to $c = \dfrac{2r\alpha(1-\alpha)}{\sin\theta}$. So the equation of our crease is

$$y\sin\theta + (\cos\theta - (1-2\alpha))x \;=\; 2r\alpha(1-\alpha). \tag{3}$$

Differentiating that last equation with respect to $\theta$, we get

$$y\cos\theta - x\sin\theta = 0 \;\Rightarrow\; \tan\theta = y/x$$

$$\Rightarrow\;\; \sin\theta = \frac{y}{\sqrt{x^2+y^2}} \;\text{ and }\; \cos\theta = \frac{x}{\sqrt{x^2+y^2}};$$

and substituting these values for $\sin\theta$ and $\cos\theta$ in equation (3) we get, after some simplification,

$$\frac{x^2+y^2}{\sqrt{x^2+y^2}} \;=\; (1-2\alpha)x + 2r\alpha(1-\alpha). \tag{4}$$

Now square equation (4), get rid of the fraction, complete the square in $x$ and then, after some simplification, we get

$$4\alpha(1-\alpha)\left[x - \frac{r}{2}(1-2\alpha)\right]^2 + y^2 \;=\; r^2\alpha(1-\alpha). \tag{5}$$

Finally, in equation (5), divide through by $r^2\alpha(1-\alpha)$, put $b^2 = r^2\alpha(1-\alpha)$,

$a^2 = r^2/4$, $x' = x - (1 - 2\alpha)/2$ (i.e. move the axes), then drop the accent and, presto, you have the standard equation of an ellipse:

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} \;=\; 1.$$

With $0 > \alpha > 1$, i.e. with $F$ outside the circle, put $-b^2 = r^2\alpha(1 - \alpha)$ and you have the equation of a hyperbola.

Now for the creation of our four-cusped curve; but first a definition. The envelope formed by the normals to a curve is called the *evolute* of the curve and it can be shown that it is also the locus of the centres of curvature of the curve at its various points. It is usually easier to find the envelope of a curve's normals than to find the locus of the centres of curvature by first finding the radius of curvature (at a general point of the curve) and then from that the coordinates of the centre of curvature of the curve at that point. Below, we show the derivation of the envelope of the normals to an ellipse. Incidentally, the Cartesian coordinates of the centre of curvature for the point $(x, y)$ on the curve $y = f(x)$ are, if they exist, given by

$$\left( x - \frac{\dfrac{dy}{dx}\left(1 + \left(\dfrac{dy}{dx}\right)^2\right)}{\dfrac{d^2y}{dx^2}},\quad y + \frac{1 + \left(\dfrac{dy}{dx}\right)^2}{\dfrac{d^2y}{dx^2}} \right).$$

With the ellipse represented by $x = a\cos\theta$, $y = b\sin\theta$, the tangent at the point with parameter $\theta$ has gradient $m' = -b\cos\theta/a\sin\theta$. Hence the gradient of the normal at that point is $m = a\sin\theta/b\cos\theta$. Substituting $x = a\cos\theta$, $y = b\sin\theta$ to find $c$ in $y = mx + c$, we get

$$\frac{ax}{\cos\theta} - \frac{by}{\sin\theta} \;=\; a^2 - b^2 \tag{6}$$

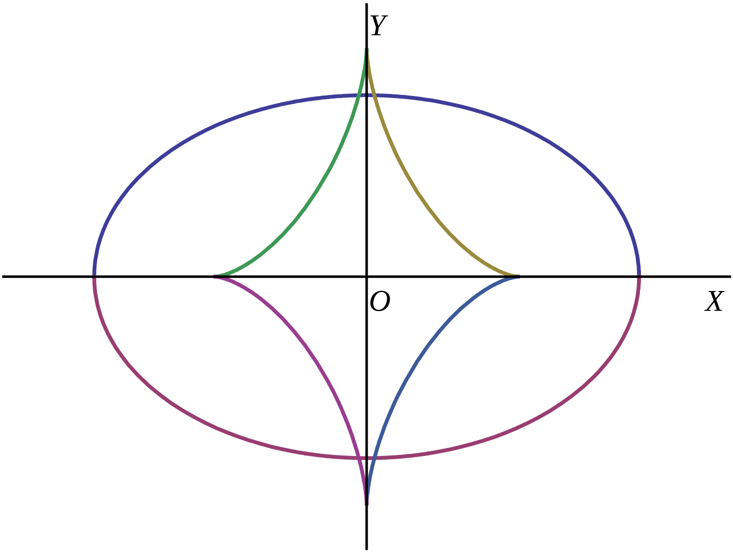
as the equation for the family of the ellipse's normals. Differentiating this equation w.r.t. $\theta$ produces, after some trigonometric manipulation,

$$\frac{\sin\theta}{\sqrt[3]{by}} \;=\; \frac{\cos\theta}{\sqrt[3]{ax}} \;=\; \frac{1}{\sqrt{(ax)^{2/3} + (by)^{2/3}}}.$$

Finally, using these values for $\cos\theta$ and $\sin\theta$ in equation (6) and yet more algebraic manipulation, we arrive at the equation of the envelope of an ellipse's normals

$$(ax)^{2/3} + (by)^{2/3} \;=\; \left(a^2 - b^2\right)^{2/3}.$$

The algebra may be a little inelegant but the resulting curve is striking.



More generally, let $\phi(x, y, \lambda) = 0$ be the equation of a family of curves, not necessarily straight lines. The equation derived by eliminating $\lambda$ from that equation and $\partial\phi(x, y, \lambda)/\partial\lambda = 0$ is called the envelope of the family.

Here's a problem set in one of the Maths Tripos exams at Cambridge a long time ago (*). A straight line meets one of a system of confocal conics in $P$ and $Q$, and $RS$ is the line joining the feet of the other two normals drawn from the point of intersection of the normals at $P$ and $Q$. Prove that the envelope of $RS$ (varying for each member of the confocal conics) is a parabola touching the axes.

A *caustic* or *caustic curve* is defined as follows. Let $C$ be a plane concave 'bright curve', i.e. a plane curve assumed to be reflective on its concave side and $P$ a point on the concave side of the curve. Then the caustic of $P$ with respect to $C$ is the envelope, if any, produced by the reflected light of the rays emanating from a point source of light at $P$. (Without requirements as to continuity and existence, this is all rather unrigorous.) For instance, we show below that the caustic of a focus of an ellipse is not a curve but a single point, the other focus. This result is illustrated by the following. Imagine an assassin standing at one of the foci in an elliptically shaped room, the wall of which is made of perfect bullet-reflecting material. If his intended victim, in the room, is not at either focus and the assassin's aim is not good, then when he fires his gun he will succeed in shooting himself.

One definition of an ellipse is the curve traced out by the locus of a point $P$ such that the sum of its distances from two fixed points, $F_1$ and $F_2$ (the foci), is constant. Let $r_1$ and $r_2$ be the lengths of the radius vectors from the foci to $P$; then the ellipse can be represented by $r_1 + r_2 = c$, a constant. With a suitable coordinate frame of reference the lengths of these radius vectors can be written as $\sqrt{(x \pm a)^2 + y^2}$ where $a$ is a constant. Let the real function $f : \mathbb{R}^2 \to \mathbb{R}$ be defined by $f(x, y) = r_1 + r_2$.

The rate of increase of $f$ in the direction of the $X$-axis is $\partial f/\partial x$ and the rate of increase of $f$ in the direction of the $Y$-axis is $\partial f/\partial y$. From this we get the vector $\nabla f = (\partial f/\partial x,\ \partial f/\partial y)$ from which it follows that the rate of increase of $f$ in the direction of the unit vector $t$ is the dot product $\nabla f \cdot t$. Differentiating $r_1 = \sqrt{(x - a)^2 + y^2}$ with respect to $x$, and then with respect to $y$, we get

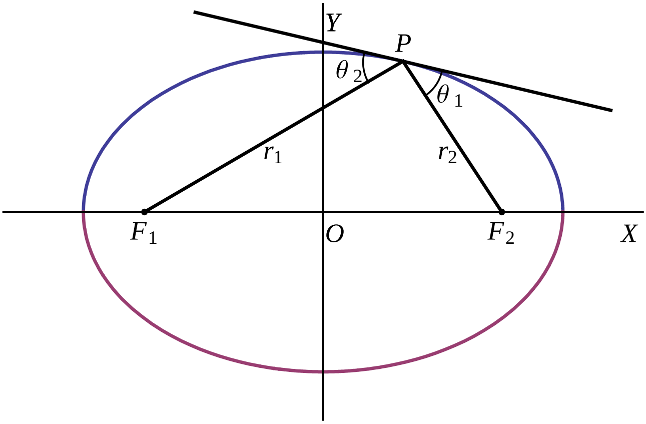
$$\nabla(r_1) \;=\; \left(\frac{x-a}{r_1}, \frac{y}{r_1}\right) \;=\; e_1,$$

the unit vector in the direction of $F_1P$. Hence $\nabla(r_1 + r_2) = e_1 + e_2$ and $\nabla f \cdot t = (e_1 + e_2)t$.

Finally, if $t$ is in the direction of the tangent to the ellipse at $P$ then, since $f$ is not increasing in that direction ($f$ is constant on the ellipse), we have $\nabla f \cdot t = 0$; i.e. $(e_1 + e_2) \cdot t = 0$; hence $e_1 \cdot t = -e_2 \cdot t$, and from this it follows that

$$\cos\theta_1 = -\cos(\pi - \theta_2) \quad \Rightarrow \quad \theta_1 = \theta_2.$$

Hence the ray from $F_1$ is reflected at the ellipse through $F_2$ and then from $F_2$ via the ellipse back through $F_1$, and the assassin has shot himself.



Here is another problem. Find the equation of the caustic resulting from a point source of light on the circumference of a reflecting circular arc, and sketch it. This caustic curve is known as a *cardioid.*

(*) 1884. Most of this piece on envelopes and caustics comes from the one text book I kept from long ago. Written in flyleaf of the book is the date of the start of my first year in the VIth form: September 1948. The book has the title *Differential Calculus*, by Joseph Edwards, M.A., and was published by Macmillan. It must have been a best seller, as far as maths books go, for the first edition was published in 1886 (!), a second edition in 1892, a third in 1896 and it was then reprinted in 1900, 1904, 1909, 1912, 1915, 1918, 1921, 1925, 1929, 1938 and, my copy, in 1948. All of which shows that I am now in my dotage.

(*Oh God. You can keep your eternity. Give me back my youth!*)

# Problem 194.1 – Normals to an ellipse

## ADF

Show that the normals drawn to the ellipse $\dfrac{x^2}{a^2}+\dfrac{y^2}{b^2}=1$ from any point on the curve

$$((a^2-b^2)^2-a^2x^2-b^2y^2)^3 \;=\; 54a^2b^2(a^2-b^2)^2x^2y^2$$

form a harmonic pencil.

This comes from the same source [*] as the one about four roots being in a harmonic ratio (Problem 190.7). We think it is appropriate for the current issue, for Bob Escolme's article, above, also features the normals to an ellipse of the same equation. Your Editor must have blinked when his school covered this topic in the A-level syllabus, so he would appreciate an explanation of the term 'pencil', harmonic or otherwise. ...

[*] E. M. Radford, *Mathematical Problem Papers*, CUP, 1904.

# Problem 194.2 – Surface area of an ellipsoid

... And to continue the elliptical theme, here's another. As any fool knows, the volume of the ellipsoid

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}+\frac{z^2}{c^2} \;=\; 1$$

is given by the elementary formula $4abc\pi/3$. But what is its surface area?

# Solution 191.1 – Bee

A bee visiting a group of flowers behaves as follows. On arriving at a flower, it drinks the nectar and moves on, unless it drank the nectar on a previous visit, in which case it moves on at once. On leaving a flower, it goes to a flower chosen at random from the whole group of flowers. It takes three seconds to drink the nectar from a flower, and one second to move from one flower to the next. Show that the expected value of the time taken to visit all the flowers is

$$\mathbb{E}(T) \;=\; n\left(4+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{n-1}\right)$$

and find $\mathbb{V}(T)$, its variance.

## David Kerr

Define random variables as follows: $X$ is the total number of visits that the bee makes to sample the nectar from all $n$ flowers; $T$ is the time required to make the $n$ visits. Clearly $T = X + 3n - 1$.

We are asked to find $\mathbb{E}(T)$ and $\mathbb{V}(T)$. It is easier to work with $X$; so the first step is to express $\mathbb{E}(T)$ and $\mathbb{V}(T)$ in terms of $X$. Since expectation is a linear function, $\mathbb{E}(T) = \mathbb{E}(X + 3n - 1) = \mathbb{E}(X) + 3n - 1$. Furthermore, $\mathbb{V}(T) = \mathbb{V}(X)$ as adding a constant term to $X$ does not change the variance.

Given that the $(r-1)$th flower has been found, the probability of finding the $r$th flower at the first attempt is

$$(n+1-r)/n. \tag{1}$$

The mean of the number of such attempts is just the reciprocal of this, $n/(n+1-r)$. Hence

$$\mathbb{E}(X) = \sum_{r=1}^{n} \frac{n}{n+1-r}. \tag{2}$$

Then

$$\mathbb{E}(T) \;=\; 3n-1+\sum_{r=1}^{n}\frac{n}{n+1-r} \;=\; n\left(4+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n-1}\right),$$

which is the required result.

To find the variance we will need to find the probability generating function of $X$. The usual custom is to express this as $\Pi_X(s)$, where the coefficient of $s^x$ gives the probability that $X = x$.

Define $X_r$ as the random variable for the number of visits required to find the $r$th flower, given that the $(r-1)$th flower $\Pi_{X_r}(s)$ has been found. Then $X = \sum_{r=1}^{n} X_r$ and, by a standard result,

$$\Pi_X(s) \;=\; \Pi_{X_1}(s)\Pi_{X_2}(s)\ldots\Pi_{X_n}(s). \tag{3}$$

But $X_r$ has a geometric distribution with $p = (n+1-r)/n$ (see (1) above), and the probability generating function is given by $ps/(1-qs)$, where $q = 1-p$. Substituting for $p$ and $q$ we get

$$\Pi_{X_r}(s) \;=\; \frac{(n+1-r)s}{n+(1-r)s}.$$

Now $\mathbb{E}(X) = \Pi'_X(1)$ and we therefore need to find $\Pi'_X(s)$. From (3) we get

$$\Pi'_X(s) \;=\; \Pi_X(s)\sum_{r=1}^{n}\frac{\Pi'_{X_r}(s)}{\Pi_{X_r}(s)}.$$

After differentiation of $\Pi_{X_r}(s)$ and some algebra we find that

$$\Pi'_X(s) \;=\; \Pi_X(s)\sum_{r=1}^{n}\frac{n}{ns+(1-r)s^2}$$

and hence

$$\mathbb{E}(X) \;=\; \Pi'_X(1) \;=\; \sum_{r=1}^{n}\frac{n}{n+1-r},$$

which confirms (2). (Note that $\Pi_X(1) = 1$.)

By another standard result,

$$\mathbb{V}(X) \;=\; \Pi''_X(1) + \Pi'_X(1) - (\Pi'_X(1))^2.$$

After a further differentiation (of $\Pi'_X(s)$) and some rather unpleasant algebra we get

$$\mathbb{V}(X) \;=\; \mathbb{V}(T) \;=\; \sum_{r=1}^{n}\frac{n(r-1)}{(n+1-r)^2}.$$

---

A Health Department census calculates that 460,000 nursing staff are currently employed by the NHS, and notes 'figures are rounded up to the nearest whole number'.—[**EK**]

---

Why is an electric kettle always non-empty? Because it contains an element.

# Solution 189.6 – Three friends

> I have three friends, Alan, Bert and Curt. I write a different positive integer on the forehead of each of them and I tell them that one of the numbers is the sum of the other two. They take it in turns in alphabetical order to attempt to deduce their own number. The conversation goes as follows. Alan: 'I cannot deduce my number.' Bert: 'I cannot deduce my number.' Curt: 'I cannot deduce my number.' Alan: 'My number is 50.' What are Bert's and Curt's numbers?

## Geoff Corris

I have enjoyed puzzling over this for some time and have come up with a possible answer—$A = 50$, $B = 40$, $C = 10$.

(1) $A$ knows he is either 50 or 30.

(2) $B$ knows he is either 40 or 60, and he also knows that neither of these answers would have helped $A$ to deduce his particular number.

(3) $C$ knows he is either 10 or 90 and cannot make any deductions.

(4) Back to $A$. If $A$ were 30, then $B$ would think he was 40 or 20. But he can't be 20 as $A$ would have been able to deduce straight away that he was 30. So $B$ must be 40 and hence $A$ knows that he must be 50.

---

**ADF**—Can someone explain why this solution differs from David Porter's answer in M500 **192**.

---

# Solution 191.7 – Sum and reciprocal

> There are $n$ positive numbers, $a_1, a_2, \ldots, a_n$. Show that
>
> $$(a_1 + a_2 + \cdots + a_n)\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}\right) \;\geq\; n^2.$$
>
> This one seems to have been quite popular! We offer a representative sample to illustrate a variety of methods and results.

## David Kerr

Multiplying out the brackets gives $n$ terms of the form $a_i/a_i$, which equals 1, and $n(n-1)/2$ terms of the form $a_i/a_j + a_j/a_i$, $i \neq j)$, which equals $2 + (a_i - a_j)^2/(a_i a_j)$ by a simple identity. This implies that $a_i/a_j + a_j/a_i \geq 2$ for $a_i, a_j > 0$. Hence the product is at least $n + 2n(n-1)/2 = n^2$.

---

## John Spencer

Here's an approach to the problem using mathematical induction, which makes the counting argument clear and easy to understand.

Let $S_n = a_1 + a_2 + ... + a_n$ and

$$R_n = \frac{1}{a_1} + \frac{1}{a_2} + ... + \frac{1}{a_n}.$$

Let $P(n)$ be the proposition that $S_n R_n \geq n^2$. Then $P(1)$ is obviously true $(a_1/a_1 = 1^2)$, and $P(2)$ holds since

$$(a_1 + a_2)\left(\frac{1}{a_1} + \frac{1}{a_2}\right) = \frac{a_1}{a_1} + \frac{a_2}{a_2} + \frac{a_1}{a_2} + \frac{a_2}{a_1} = 2 + \frac{a_1^2 + a_2^2}{a_1 a_2}$$

$$= 2 + \frac{(a_1 - a_2)^2 + 2a_1 a_2}{a_1 a_2} = 4 + \frac{(a_1 - a_2)^2}{a_1 a_2} \geq 2^2.$$

Assume $P(k)$ (induction hypothesis). Then

$$S_{k+1} R_{k+1} = S_k R_k + a_{k+1} R_k + \frac{S_k}{a_{k+1}} + \frac{a_{k+1}}{a_{k+1}}$$

$$= S_k R_k + \left(\frac{a_{k+1}}{a_1} + \frac{a_{k+1}}{a_2} + ... + \frac{a_{k+1}}{a_k}\right) + \left(\frac{a_1}{a_{k+1}} + \frac{a_2}{a_{k+1}} + ... + \frac{a_k}{a_{k+1}}\right) + 1.$$

Each fraction in the first set of brackets can be paired with its inverse in the second set of brackets, to give

$$= S_k R_k + \left(\frac{a_{k+1}}{a_1} + \frac{a_1}{a_{k+1}}\right) + \left(\frac{a_{k+1}}{a_2} + \frac{a_2}{a_{k+1}}\right) + ... + \left(\frac{a_{k+1}}{a_k} + \frac{a_k}{a_{k+1}}\right) + 1,$$

with $k$ pairs of fractions each greater than or equal to 2, as shown above for $a_1/a_2 + a_2/a_1$. Accordingly,

$$S_{k+1} R_{k+1} \geq S_k R_k + 2k + 1.$$

By the induction hypothesis $S_k R_k \geq k^2$; so

$$S_{k+1} R_{k+1} \geq k^2 + 2k + 1 = (k+1)^2.$$

And $P(k)$ implies $P(k+1)$. But $P(2)$ holds, so the proposition applies for all values of $n$ by mathematical induction.

## John Bull

The result follows from the inequalities $A \geq G \geq H$ involving the arithmetic, geometric and harmonic means, where

$$A = \frac{1}{n}(a_1 + a_2 + \cdots + a_n), \quad \frac{1}{H} = \frac{1}{n}\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}\right).$$

They can be found in the *Schaum Mathematical Handbook.* There are proofs in classic texts such as those of G. H. Hardy and J. W. Archbold, but they appear to be rare in modern books (at least those of moderate cost).

---

## Mike Lewis

*Solution 1*

The Cauchy–Schwarz inequality states that

$$\sum_{k=1}^{n}(v_k^* w_k) \sum_{m=1}^{n}(v_m^* w_m) \leq \sum_{k=1}^{n}(v_k^* v_k) \sum_{m=1}^{n}(w_m^* w_m),$$

or in another form for purely real values of $v$ and $w$,

$$\begin{aligned}(v_1 w_1 + v_2 w_2 + \cdots + v_n w_n)^2 \\ \leq (v_1^2 + v_2^2 + \cdots + v_n^2)(w_1^2 + w_2^2 + \cdots + w_n^2).\end{aligned}$$

Set $a_k = v_k^2 = 1/w_k^2$. Substitute to give

$$(1 + 1 + \cdots + 1)^2 \leq (a_1 + a_2 + \cdots + a_n)\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}\right).$$

Since the LHS equals $n^2$, the original statement has been proven.

*Proof of the Schwarz inequality*

Assume that $f$ is complex and there is a complex constant, $\lambda$, such that $f_k = v_k + \lambda w_k$. Since $f_k^* f_k \geq 0$, $\sum_{k=1}^{n} f_k^* f_k \geq 0$. This can be expanded as

$$\sum_{k=1}^{n}(v_k^* v_k + \lambda v_k^* w_k + \lambda^* w_k^* v_k + \lambda^* \lambda w_k^* w_k) \geq 0.$$

Now define

$$\lambda = -\frac{\sum_{k=1}^{n} w_k^* v_k}{\sum_{k=1}^{n} w_k^* w_k}, \qquad \lambda^* = -\frac{\sum_{k=1}^{n} w_k v_k^*}{\sum_{k=1}^{n} w_k^* w_k}.$$

Eliminate the $\lambda$s to obtain

$$\sum_{k=1}^{n}(v_k^* v_k)\sum_{m=1}^{n}(w_m^* w_m)-\sum_{k=1}^{n}(v_k^* w_k)\sum_{m=1}^{n}(w_m^* v_m)$$
$$-\sum_{k=1}^{n}(w_k^* v_k)\sum_{m=1}^{n}(v_m^* w_m)+\sum_{k=1}^{n}(w_k^* v_k)\sum_{m=1}^{n}(w_m v_m^*) \;\geq\; 0,$$

which simplifies to the general form of the Schwarz inequality,

$$\sum_{k=1}^{n}(v_k^* w_k)\sum_{m=1}^{n}(w_m^* v_m) \;\leq\; \sum_{k=1}^{n}(v_k^* v_k)\sum_{m=1}^{n}(w_m^* w_m).$$

*Solution 2*

Another longer but valid solution using induction is as follows.

Step 1. Clearly the statement is true for $n = 1$.

Step 2. Show that the statement is true for $n = 2$. Use proof by contradiction. Start from the statement

$$(a_1 + a_2)\left(\frac{1}{a_1} + \frac{1}{a_2}\right) \;<\; 4.$$

This denies that which is to be proved. If this statement is true then the statement we are trying to prove is false

Multiplying out gives $2 + a_2/a_1 + a_1/a_2 < 4$, which rearranges to $a_1^2 - 2a_1a_2 + a_2^2 \;<\; 0$. Factorizing the LHS, we obtain $(a_1 - a_2)^2 < 0$. The statement is clearly impossible for all values of the $a$s and thus proves that the statement

$$(a_1 + a_2 + \cdots + a_n)\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}\right) \;\geq\; n^2$$

is true for $n = 2$. It has also been proved that

$$\frac{a_2}{a_1} + \frac{a_1}{a_2} \;\geq\; 2.$$

Step 3. Show that the statement is true for all $n > 2$. When the two brackets are multiplied there will be $n^2$ terms of the form $a_i/a_j$. These terms can be grouped into $n^2/2$ pairs of the form $a_i/a_j + a_j/a_i$. It has already been proven that $a_2/a_1 + a_1/a_2 \;\geq\; 2$. For $n^2/2$ pairs, then, the sum must be at least $2n^2/2$. Since $2n^2/2$ equals $n^2$, we have completed the proof of the statement

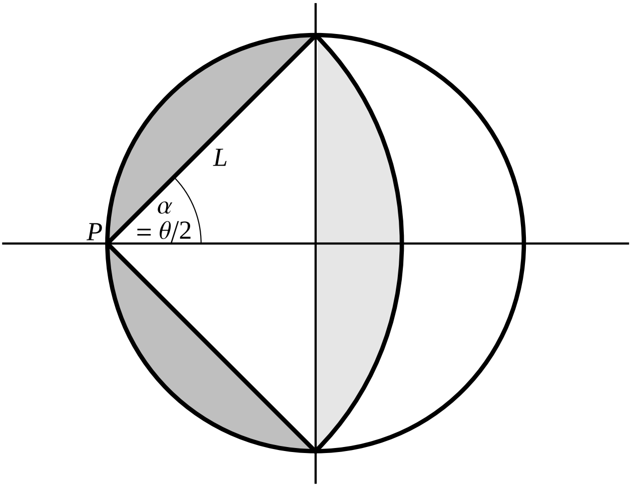
$$(a_1 + a_2 + \cdots + a_n)\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}\right) \;\geq\; n^2.$$

# Solution 191.6 – Porthole

> Consider a circular porthole of radius $r$. One end of a windscreen wiper of length $L$ is attached to a point on the circumference, and the wiper arm turns on this point, thereby sweeping out a circular sector on the porthole. This sector is half the area of the porthole. How long is the wiper?

## John Spencer

Make a unit circle centred at the origin, with the windscreen wiper attached at the point $(-1, 0)$.



The free end of the wiper touches the circle at the points $(\cos\theta, \sin\theta)$, $(\cos\theta, -\sin\theta)$; so

$$L^2 \;=\; (1+\cos\theta)^2 + \sin^2\theta \;=\; 2 + 2\cos\theta$$

and the area swept is

$$A \;=\; L^2\tfrac{\theta}{2} \;=\; \theta(1+\cos\theta),$$

since the angle subtended by a chord at the circumference is half that subtended at the centre of the circle. Putting $a = \pi/2$ gives

$$2\theta(1+\cos\theta) \;=\; \pi.$$

This has an infinite number of solutions, two in the range $0 < \theta < \pi$, but the most interesting occurs when $\theta = \pi/2$, when the free end of the wiper touches the circle at $(0,1)$ and $(0,-1)$. So the wiper sweeps half the screen area when $L = \sqrt{2}$, as shown in the diagram.

It follows that if we divide the circle vertically into two semi-circles along the diameter joining the points of contact, the area of the wiper's arc which lies in the right-hand semicircle must equal the area it leaves untouched in the left-hand semicircle.

A square inscribed in a unit circle occupies an area of 2 square units so the four crescent-shaped chord segments outside the square have an area of $\pi - 2$ units. A square inscribed in a circle of radius $\sqrt{2}$ has an area of 4 square units, so the four crescent-shaped segments in that circle have a total area of $2\pi - 4$. Their area is twice that of the corresponding parts of the smaller circle.

Consequently, the two crescent-shaped pieces left on either side of the wiper's arc (dark grey in the diagram) are the same area as the crescent-shaped segment of the wiper's arc (light grey) which lies in the right-hand semicircle.

The wiper also wipes half the screen when $\theta = \pi/3$, with $L = \sqrt{3}$. This corresponds to a longer wiper sweeping a narrower arc.

The wiper sweeps a maximum area when $dA/d\theta = 0$,

$$\frac{dA}{d\theta} = 1 + \cos\theta - \theta\sin\theta,$$

which occurs when $\theta = 1.3065$, so that the wiper sweeping the maximum area has length

$$L = \sqrt{2 + 2\cos 1.3065} = 1.5882.$$

A wiper of this length sweeps an area of 1.6478 square units.

---

**Correction** In M500 **193**, 'Solution 190.7 – Four roots', it seems that our up-down orientation became confused. The roots of the equation

$$x^4 - ax^3 + bx - b^2/a^2 = 0$$

should have been printed as

$$\sqrt{\frac{b}{a}},\ -\sqrt{\frac{b}{a}},\ \frac{a - \sqrt{a^2 - 4b/a}}{2} \text{ and } \frac{a + \sqrt{a^2 - 4b/a}}{2}$$

on page 20, and as

$$\frac{a^{3/2} - \sqrt{a^3 - 4b}}{2\sqrt{a}},\ \frac{a^{3/2} + \sqrt{a^3 - 4b}}{2\sqrt{a}},\ -\sqrt{\frac{b}{a}} \text{ and } \sqrt{\frac{b}{a}}.$$

on page 21. Apologies to David Porter and Dick Boardman. — **ADF**

# Solution 191.6 – Porthole

## David Singmaster

Let $\alpha$ be half the angle of the sector at $P$. Then the area $S$ of the sector wiped out is $S = \alpha L^2$. We have also $L = 2\cos\alpha$, so $S = 4\alpha\cos^2\alpha$ and the relative area, $T$, is

$$T \;=\; \frac{S}{\pi} \;=\; \frac{4}{\pi}\,\alpha\cos^2\alpha.$$

Setting $T = 1/2$ gives us $\alpha\cos^2\alpha = \pi/8$, which has the solutions $\alpha = \pi/6$ and $\alpha = \pi/4$.

The unusual simplicity of these solutions intrigued me and I wondered if there were any similar equations with such simple roots. Examining $F(\alpha) = \alpha^a\cos^b\alpha$ for $\alpha = \pi/6, \pi/4, \pi/3$, the only repeated function values with positive exponents are for $b = 2a$, when $F(\pi/6) = F(\pi/4)$.

More generally, examination of

$$F(\alpha) = \alpha^a(\cos^b\alpha)(\sin^c\alpha)$$

for the same values of $\alpha$ reveals only three cases with repeated function values and some positive exponents:

$$\begin{array}{lll} b \;=\; 2a, & c \;=\; 0, & F(\pi/6) \;=\; F(\pi/4); \\ a \;=\; 0, & b \;=\; c, & F(\pi/6) \;=\; F(\pi/3); \\ b \;=\; c \;=\; 2a, & & F(\pi/4) \;=\; F(\pi/3). \end{array}$$

Extending the range of $\alpha$, we find another case:

$$c \;=\; 2a, \qquad b \;=\; 0, \qquad F(2\pi/3) = F(\pi/2).$$

Each of these is the simplest case of a family of solutions; for example,

$$b = 2(d+1)a, \quad c = -2da, \quad F\left((6m\pm 1)\,\frac{\pi}{6}\right) = F\left((6m\pm 1)\,3^d\,\frac{\pi}{4}\right),$$

but the first three cases are the only ones having two angles in the first quadrant.

Maximizing $T$ leads directly to $\alpha\tan\alpha = 1/2$. Using the iteration formula $\alpha_{i+1} = \tan(1/2\alpha_i)$, I obtained $\alpha \approx 0.6532711871 \approx 37.42968189°$, giving $L \approx 1.588199729$ and $T \approx 0.5245101134$.

The problem appeared, with my solution, in *Math. Gaz.* **76** (No. 477) (Nov. 1992), 453 & **77** (No. 479) (Jul. 1993), 293–294. In the published solution, Nick Lord showed that $T = 1/2$ is the only rational $T$ for which both solutions are a rational number of degrees.

# One-edge connections

You have an infinitely large sheet of squared graph paper. Step 0: select a square somewhere on the sheet and label it '0'. Step $x$: select all unlabelled squares that connect only on one edge with labelled squares; label them '$x$'.

What is the formula for the total number of labelled squares, $S(x)$, as a function of the step number, $x$?

## Ted Gore

I approached the problem by defining $r(x)$ as the number of occurrences of the symbol $x$ in the diagram, so that

$$S(x) \;=\; \sum_{i=0}^{x} r(i). \tag{I}$$

I wrote a program to calculate $r(x)$ for a range of values by just slogging through; I reproduce a portion below.

| $x$ | $r(x)$ | | | | |
|---|---|---|---|---|---|
| 16 | 4 | 16 | 64 | 256 | $1024 = 2^{10}$ |
| 17 | 12 | | | | |
| 18 | 12 | 48 | | | |
| 19 | 36 | | | | |
| 20 | 12 | 48 | 192 | | |
| 21 | 36 | | | | |
| 22 | 36 | 144 | | | |
| 23 | 108 | | | | |
| 24 | 12 | 48 | 192 | 768 | |
| 25 | 36 | | | | |
| 26 | 36 | 144 | | | |
| 27 | 108 | | | | |
| 28 | 36 | 144 | 576 | | |
| 29 | 108 | | | | |
| 30 | 108 | 432 | | | |
| 31 | 324 | | | | |

By inspection of the table I deduced the following:

$$\begin{array}{lcll}
r(2^p) & = & 4 & \text{for } p \geq 0, \\
r(2n+1) & = & 3r(2n) & \text{for } n \geq 1, \\
r(2^p+4k) & = & r(2^p+k) & \text{for } k \geq 0 \text{ and } 2^p+4k < 2^{p+1}, \\
r(2^p+4k+2) & = & 3r(2^p+4k) & \text{for } k \geq 0 \text{ and } 2^p+4k+2 < 2^{p+1}.
\end{array}$$

A slight rearrangement gives

$$\begin{aligned} r(2^p+4k) &= r(2^p+k), \\ r(2^p+4k+1) &= 3r(2^p+k), \\ r(2^p+4k+2) &= r(2^p+k), \\ r(2^p+4k+3) &= 3^2 r(2^p+k). \end{aligned}$$

Adding Mike Warburton's equation $S(2^p) = \frac{4}{3}2^{2p} + \frac{11}{3}$, from M500 **188**, page 11, $S(x)$ can be calculated recursively using

$$S(x) = S(x-1) + r(x). \tag{II}$$

I don't know how Mike arrived at his equation but from the table I noticed that

$$\sum_{i=2^p}^{2^{p+1}-1} r(i) = 2^{2(p+1)}, \tag{III}$$

so that

$$S(2^p) = r(0) + \sum_{i=1}^{p} 2^{2i} + r(2^p) = 1 + \sum_{i=1}^{p} 2^{2i} + 4 = \frac{4}{3}2^{2p} + \frac{11}{3}.$$

One further observation leads to a different approach to calculating $S(x)$. Using the extract from the table as an example, I notice that

$$\sum_{i=24}^{31} r(i) = 3\sum_{i=16}^{23} r(i), \quad \sum_{i=20}^{23} r(i) = 3\sum_{i=16}^{22} r(i) \quad\text{and}\quad \sum_{i=28}^{31} r(i) = 3\sum_{i=24}^{27} r(i).$$

The pattern continues down to the level of a single pair of $r(x)$s. We can therefore calculate $S(x)$. Let

$$S(x) = S(2^p-1+k) = S(2^p-1) + F(q(k)), \tag{IV}$$

where $k \in [1, 2^p]$ and $F$ and $q$ are defined as follows.

First, $q$ is a string of characters, $L$ and $R$, representing the position of $k$ in the interval $[1, 2^p]$. For example, to compute $q(6)$ when $p = 4$, we observe that $6 \in [1, 8]$, the left half of $[1, 16]$, $6 \in [5, 8]$, the right half of $[1, 8]$, $6 \in [5, 6]$, the left half of $[5, 8]$, and 6 is in the right half of $[5, 6]$. So $q(6) = LRLR$.

Now

$$F(A_1A_2\dots A_n) = \frac{w}{4}\sum_{i=1}^{n} f_i(A_1A_2\dots A_i) + wg(A_1A_2\dots A_n),$$

where $w = \sum_{i=2^p}^{2^{p+1}-1} r(i) = 2^{2(p+1)}$. Thus

$$\begin{aligned}
f_i(A_1A_2\dots A_i) &= 0 && \text{if } A_i = L,\\
f_i(A_1A_2\dots A_i) &= g(A_1A_2\dots A_{i-1}) && \text{if } A_i = R,\\
g(A_1A_2\dots A_n) &= \tfrac{1}{4}g(A_1A_2\dots A_{n-1}) && \text{if } A_n = L,\\
g(A_1A_2\dots A_n) &= \tfrac{3}{4}g(A_1A_2\dots A_{n-1}) && \text{if } A_n = R,\\
g(\ ) &= 1.
\end{aligned}$$

In the definition of $F$ the first term on the right of the equation represents $\sum_{2^p \le i < k} r(i)$ and the second term represents $r(k)$.

Returning to the example with $p = 4$ and $k = 6$, we have $q(6) = LRLR$ and

$$\begin{aligned}
F(LRLR) &= \frac{w}{4}\left[f_1(L) + f_2(LR) + f_3(LRL) + f_4(LRLR)\right] + wg(LRLR)\\
&= \frac{w}{4}\left[0 + g(L) + 0 + g(LRL)\right] + w\cdot\frac{3}{4}\cdot\frac{1}{4}\cdot\frac{3}{4}\cdot\frac{1}{4}\\
&= \frac{w}{4}\left[\frac{1}{4} + \frac{1}{4}\cdot\frac{3}{4}\cdot\frac{1}{4}\right] + \frac{9w}{256} = \frac{28w}{256} = 112,
\end{aligned}$$

since $w = 1024$. So

$$\begin{aligned}
S(21) &= S(15+6) = S(15) + F(q(6))\\
&= 1 + \frac{4}{3}\left[(2^4)^2 - 1\right] + 112 = 453
\end{aligned}$$

(using $r(0) = 1$ and (III)), which agrees with the value found by the recursive equation (II).

Summing up, we obtain, for $k \in [1, 2^p]$,

$$\begin{aligned}
S(2^p - 1 + k) &= S(2^p - 1) + F(q(k))\\
&= \frac{1}{3}\left[4(2^p)^2 - 1\right] + F(q(k)).
\end{aligned}$$

If $k = 1$, then $F = 4$ and this reduces to

$$\frac{4}{3}2^{2p} + \frac{11}{3}.$$

---

A man and a woman are talking. The man's mother-in-law is the woman's mother-in-law's mother.

How are they related? — [**EK**]

# A method of solving Vigenere ciphers

## Dick Boardman

With M500 **192**, members received a CD ROM promoting Simon Singh's *The Code Book*. In his book and on the disk, Singh gives the classic Kasiski method of solving Vigenere ciphers. There is however another simple, though rather laborious, method which does the job even more effectively. Imagine the letters of a piece of text arranged in a single long string, written along a single line. Now duplicate the string and position it exactly underneath the first. Each letter is now above a copy of itself and so the number of matching letter pairs equals the number of letters in the whole text. Now shift the lower string one letter space to the right. The number of places where the letters match drops dramatically but is not usually zero in a long text, and shifting the strings $2, 3, 4, \ldots$ places produces about the same result.

Applied to a random string of letters, this would produce a uniform average value of coincidences of 1/26.

Applied to a string of English text the result is much higher but still fairly uniform. This is because English has a well-defined letter frequency pattern with E, T, A, O, I, N, S, H, R, D, L, U being the most common letters, in that order, and certain letter pairs, triplets and so on are used more often than others, 'THE' and 'AND' being common examples.

If you apply this technique to a piece of text which has been ciphered in a simple, monoalphabetic cipher, the result is exactly the same! Each plaintext letter is always replaced by the same cipher letter and so the number of coincidences is exactly the same.

But apply this technique to a piece of text which has been ciphered in a Vigenere cipher and the result is very different. Firstly, for most shifts, the number of coincidences is much smaller, close to 1/26. This is because the letter frequency pattern and the frequency of letter pairs and triplets is disrupted. However, every so often you get a much higher frequency, and these higher values are always the same number of shifts apart. This number of shifts is the length of the Vigenere code word. This works because, whenever the number of shifts is a multiple of the length of the code word, each letter is compared to another letter in the same substitution alphabet. The method includes the Kasiski method since repeated strings of letters, separated by multiples of the length of the keyword will increase the number of coincidences substantially.

Once the length of the keyword has been established, the method of solution is the same as for the Kasiski method. Break the text into $n$ groups of letters, where $n$ is the length of the keyword. Do a frequency analysis on each group and assume that the most common letter is E, or T, or A, and look to see if a keyword emerges. Then work backwards to the original text.

As an illustration of the power of these techniques, I applied them to the Vigenere example in the challenge section of Singh's book. The shifting technique quickly established that the keyword was five letters long and frequency analysis showed that it was 'SCUBA' which, strictly speaking, is an acronym rather than a word. I worked back to the original text and found that it wasn't English but French. I don't speak French, having been taught German at school, but friends assured me that it was good, accurate French. Thus these methods had allowed me to decipher a text in an unknown language which I do not speak! I can only assume the E is the most common letter in both English and French.

I found this method in the first edition of David H. Kahn's classic book, *The Codebreakers.* Later editions are shorter and don't include it and I have never seen it in any other book. It is similar to the technique called autocorrelation, which finds hidden periodicities in noisy time sequences. Although Kahn does not say so, I suspect that the method has much wider application and can be used to identify the language and type of other ciphers and also to help solve them.

# Forty

## Eddie Kent

If I were to ask you what is special about the number 29 you would almost certainly answer that it is the only number that tells you how many straight lines is is made from. So I won't. However, can you tell me what is special about 40?

(Anyone who has read Steve Ainley's book, *Mathematical Puzzles*, should have no trouble with this.)

# Prime primes

## Eddie Kent

A *prime prime* is a prime number from which successive right-hand digits can be stripped off, leaving a prime number at each step. Can you find the largest one. It will probably be eight digits long.

# Solution 191.9 – Switch

> Formulate a strategy which will guarantee a win for the contestants in the following game.
>
> The game involves a host $H$, a switch $S$ (with two settings: ON/OFF), and $n$ contestants. Initially $H$ sets $S$ one way or the other. The game then proceeds in stages. At each stage, $H$ chooses a contestant $C$, who can either (i) change the setting of $S$, or (ii) leave $S$ unchanged, or (iii) announce that all $n$ contestants have been chosen by $H$. The game continues until case (iii) occurs, when the game ends. The contestants win if and only if $C$'s assertion is true. The rules are: (a) the contestants may consult with each other before the game begins; (b) no communication (other than via $S$) is allowed after the game has started; (c) if the game goes on for ever, each contestant will be chosen infinitely often.

## Dick Boardman

I am not clear whether you have a solution or whether you are inviting readers to construct a puzzle.

I introduce the following extra assumptions, which I think make the solution as difficult as possible.

(1) Contestants do not know the initial setting of the switch.

(2) Contestants are called at irregular intervals of time and do not know if any other contestant has been called in the meantime.

(3) The host may call any contestant at any time and may actively disrupt any contestant scheme.

The simplest case is for two contestants. This is solved if they agree as follows. Contestant $A$ will note the position of $S$ when she is called and, if it is OFF move it to ON. Contestant $B$ will note the position when she is called and, if it is ON move it to OFF.

The first time a contestant is called, she will not know the initial position of the switch, or whether her partner has been called yet so all she can do is carry out her operation. However, if on any subsequent call the switch is not as she left it, she may claim. The host may delay the result as long as she wishes by calling $ABBBBBBBBBB\ldots$ but to comply with the second rule, must eventually call $A$ again and lose.

Three contestants is more difficult.

The best I can do is for $A$ and $B$ to act as before and $C$ to act as a watcher, never moving the switch. Only $C$ may claim and she may claim whenever she sees that the switch has moved twice. However, This fails if the host always calls $ABCABCABC\ldots$, which complies with rule (b). To make this work, we must modify my rule (3) to say that the host must call the contestants in random order. I suspect that a solution is also possible if contestants are told whenever someone (they don't know who) has been called. Can anyone else do any better?

# Goat

## John Spencer

In the discussion of Problem 190.3 (Goat), you asked for a more elegant solution of the circular barn case. [There is a circular barn of radius $r$ in the middle of a field. A goat is tethered to a point on the outside of the barn by a rope of length $\pi r$. What area of field can the goat reach?] I can't tell whether this is a more elegant solution, but it avoids square roots of quadratic functions.

The semicircular area formed by the tangent to the barn at the point of attachment of the tether has area $\pi^3 r^2/2$. The remainder of the grazeable area can be found by considering the situation where the goat is at the end of its tether and the amount of the tether which is taut against the barn wall subtends an arc of length $\theta r$. Then let the goat move round towards the back of the barn by a small amount so that the arc subtended now has length $(\theta + \delta\theta)r$.

The tangents at $\theta$ and $\theta + \delta\theta$ can be seen to form a triangle, whose sides are $(\pi - \theta)r$ and $\pi - (\theta + \delta\theta)r$ and in which the angle between the two long sides is $\delta\theta$. The area of this triangle is $r^2/2 \cdot (\pi - \theta)(\pi - (\theta + \delta\theta))(\sin\delta\theta)$. If $\delta\theta$ becomes very small, this expression simplifies to $r^2(\pi - \theta)^2\delta\theta/2$, since $\sin\delta\theta \to \delta\theta$ and the term in $\delta\theta\delta\theta$ can be ignored.

This can be integrated between $\theta = 0$ and $\theta = \pi$, then doubled to give the area the goat can graze along the sides of the barn.

$$r^2 \int_0^\pi (\pi - \theta)^2 d\theta \;=\; \frac{r^2\pi^3}{3}.$$

Adding the semicircle gives a total area of

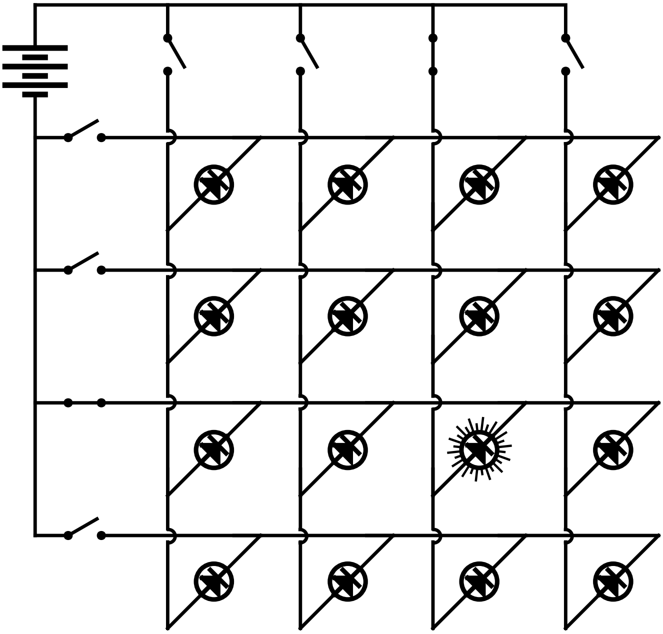
$$\frac{r^2\pi^3}{2} + \frac{r^2\pi^3}{3} \;=\; \frac{5}{6}\pi^3 r^2.$$

## Solution 190.5 – Eight switches

> Using a battery, wire, light bulbs and eight on–off switches, construct a circuit that allows you to control as many lights as possible. You should be able to select a single bulb and switch it on while all the others remain unlit. What if you use LEDs?

**Dick Boardman** sent this diagram showing how to control 16 light-emitting diodes. It is clear that the diode at position $(r, c)$, and only that diode, is illuminated by closing just the switch at row $r$ and the switch at column $c$. This is illustrated for (3, 3).

Notice that the circuit won't work for ordinary light bulbs because they allow current to flow in either direction. (See page 28.)



We would still like to see either a circuit that controls more than 16 LEDs, or a proof that no such thing exists.

Where there's a will there's a way. Fine words butter no parsnips. When the cat's away, the mice will play. Half a loaf is better than no bread. It's an ill wind that blows nobody any good. Red sky at night is the shepherd's delight; red sky in the morning is the shepherd's warning. Don't spoil the ship for a ha'porth of tar. A rolling stone gathers no moss.

# Letters to the Editors

## Proverbs

Dear Eddie

Many thanks for M500 **192**. My respect to David Porter for solving 'Three friends'. I had examined those numbers myself and had failed to get the next step. Problem 192.3—Platonic solids—is reminiscent of Kepler's idea that the spacing of the planets from the sun was governed by Platonic solids of increasing complexity fitted inside each other, though in this case I think they were inscribed within spheres and there was no fitting problem. Problem 192.5—16 polygons—seems to have a non-solution on the cover. You never caption your covers; maybe you ought to. Not having come up with a solution to this (the only one that looks faintly possible), I am sending some more proverbs, of which you will probably have a surplus anyway.

Best wishes,

**Ralph Hancock**

---

1. A 50 per cent issue of a standard wheat-based oven-processed nutritional unit will attract a higher customer preference rating than such an issue having identical parameters other than that the percentage is zero.

2. Totally non-beneficial airflow is negatively perceived.

3. The frequency shift of incident solar radiation towards the longer wavelengths of the visible spectrum, occurring in temporal proximity to the termination of the daylight period, was found to strongly stimulate the pleasure centres of ovine management operatives. In sharp contrast to this finding, when a comparable celestial phenomenon was observed shortly after the commencement of the daylight period, these operatives experienced feelings of anxiety.

4. Volition entails facilitation.

5. The conduct of high-level one-on-one verbal interchange has zero correlation with high-fat dairy spread migration to a *Pastinaca sativa* substrate.

6. Constant rotation of a rock fragment is inimical to bryophyte colonization.

7. It is ill advised to court the downgrading of a vessel's seaworthiness rating through underspending to the value of £0.00208333 . . . on the application of a long-chain hydrocarbon preservative.

8. Feline proximity is inversely related to ludic behaviours in rodents.

---

## Fermat numbers

Tony,

I had a go at working out the volume required to house the 2145351st Fermat number [M500 **192**, p. 16].

If you use both sides of the paper, I worked out that the print density would be about $2 \cdot 10^9$ digits per cubic metre, E&OE. But whether that is right or not becomes irrelevant if the 645815-digit figure was an approximation. For instance, if you work to four figures, and say that the number of digits is between $10^{645800}$ and $10^{645900}$, the error created by this uncertainty makes the print density of $2 \cdot 10^9$ irrelevant. Then, as there are only $8.46787 \cdot 10^{47}$ cubic metres in a cubic light-year, using cubic light-years instead of cubic metres makes little difference, because of the uncertainty.

The number of elementary particles in the universe has been estimated as less than $10^{90}$, and as each digit would require more than one elementary particle to express it, it looks as if one would need at least $10^{645000}$ universes to house the book of numbers.

When the book has been produced, its mass will be >>> than the mass of any known astronomical object, so it will immediately undergo gravitational collapse. As it is so big, and as it presumably cannot collapse faster than the speed of light, for practical purposes the collapse will carry on for the rest of time. The resulting supernova will be spectacular.

**Colin Davies**

---

**ADF** writes — Let $D$ denote the number of digits in $F_{2145351} = 2^{2^{2145351}} + 1$. What I said in M500 **192** was that $D$ has approximately 645815 digits. Actually this is an extremely good approximation. It is exact. Furthermore it is even possible to calculate $D$ itself without error. Since $(\log F_{2145351})/(\log 10)$ is not too near an integer, the difference between $F_{2145351}$ and $F_{2145351} - 1$ can be safely ignored. Therefore we have $D = \lceil(\log F_{2145351})/(\log 10)\rceil = \lceil 2^{2145351}(\log 2)/(\log 10)\rceil = 3025780990\ldots0163382946 \approx 3.025780990 \cdot 10^{645814}$, and if you are really interested I can show you the entire exact value—all 645815 digits of it.

Dividing $D$ by $1.410 \cdot 10^{57}$, approximately the number of digits one can store in a cubic light-year of M500 pages, gives a reasonable estimate for the volume of the magazine: $2.145 \cdot 10^{645757}$ cubic light-years.

---

*Correction.* In case you didn't notice, $F_1$ is equal to 5, not 3.

## All the sevens

Dear Tony,

On page 13 of M500 **192**, two solutions are given to Problem 189.7, which asked for a proof that, for any non-negative integer $N$, the last digit of $N^{77}$ is the same as the last digit of $N$. You appended a 'Note to experts' stating that 'Those of you who are number-theoretically well educated know that it is possible to deliver the answer in one or two lines. In fact all you need to do is utter the words "Fermat's Little Theorem" and maybe "Euler's totient function" ....'

I should be interested to know more because, while I cannot claim to be 'number-theoretically well educated', I did struggle through M381 about ten years ago and one of the few things I remember from it is Fermat's beautiful theorem. A condition for it to apply is that $P$, the power to which the integer is raised, must be prime which 77 ($= 7 \cdot 11$) clearly is not. My memories of Euler's extension to Fermat's theorem are vaguer but reference to page 142 of Burton's *Elementary Number Theory* confirms that a condition for Euler's theorem to apply is that $W$, the argument of the totient function to which the integer $N$ is raised, must be relatively prime to $N$. In the case of the problem under consideration, this means that $W$, whatever it is, must be such that $\phi(W) = 77$ and that $\gcd(W, N) = 1$. This cannot be the case for all integer values of $N$ since these include all multiples of $W$ and its prime factors.

Best wishes,

**Patrick Lee**

---

**ADF** writes — As far as I can recall, I was probably thinking along the following lines. Since $\phi(10) = 4$, we have, by Fermat's Little Theorem, $N^4 \equiv 1 \pmod{10}$; hence $N^{77} \equiv NN^{76} \equiv N \pmod{10}$.

Unfortunately I forgot that this is valid only for $N$ co-prime to 10, i.e. $N \equiv 1, 3, 7$ or $9 \pmod{10}$.

Alternatively, one can argue thus. Since $\phi(5) = 4$, we have $N^{77} \equiv N(N^4)^{19} \equiv N \pmod 5$. This holds by FLT for $N$ not divisible by 5, and trivially otherwise. Similarly, since $\phi(2) = 1, N^{77} \equiv N \pmod 2$. We can combine the results to get $N^{77} \equiv N \pmod{2 \cdot 5}$. This is valid because 2 and 5 are co-prime.

So 'one or two lines' was a hideous exaggeration. A slap on the wrist is in order.

## Marks

I am not sure that I agree with this but I thought you might be interested. It came up on a maths page on the Internet.

A maths teacher gives her students an exam with 100 true-or-false questions. Arthur gets all 100 correct; Ford gets 50 correct; Marvin gets 100 wrong. After thinking about their results, the teacher decides to give her students a score that indicates their true knowledge of the subjects covered by the test. What did each student score?

Marvin gets 100 for it is nearly impossible to guess and get them all wrong, he must have known the correct answers. Arthur knew them all so he gets 100. Ford obviously guessed, so he gets 0.

**Ron Potkin**

# Problem 194.3 – Sixteen lamps

## ADF

Refer to the circuit diagram on page 24. Now suppose that the diodes are replaced by ordinary lamps. For definiteness, let the battery have 1 volt and the lamps 1 ohm resistance each.

Can you calculate the currents that flow through the various lamps? Alternatively, perhaps there is someone who might like to build the actual circuit and make the appropriate measurements. Either way, we would be most interested in the results.

# Problem 194.4 – Getting dressed

## ADF

Your wardrobe consists of $h$ hats, $b$ bras, $p$ pairs of panties, $d$ dresses, $s$ pairs of socks and $f$ pairs of shoes.

In how many ways is it possible for you to get properly dressed? Assume the usual conventions:

(i) you wear one of each type of clothing;

(ii) underwear goes on before dress, and sock before shoe;

(iii) socks and shoes are paired;

(iv) chirality is relevant for shoes (but not socks).

*Question.* What is the square root of 69? *Answer.* Eight something.

# Problem 194.5 – Cube

## JRH

Imagine a $3 \times 3 \times 3$ cube. What is the longest path you can make by moving around the cube up, down, left, right, forward and backward $(U, D, L, R, F, B)$ with the following two rules?

(1) You can't go into the same $1 \times 1 \times 1$ cube twice.

(2) You can't make the same move twice in succession. (For example, $UU$ is not allowed.)

If you find the problem as stated too difficult, we suggest you try it first with a $4 \times 4 \times 4$ cube.

# What's missing?

What's missing in the following sequences?

(i) 4, 2, 3, 4, 6, 2, 3, 9, **?**

(ii) sextillion, septillion, octillion, nonillion, decillion, **?**, **?**, **?**, ..., **?**, ...

(iii) 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, **?**, 347, 349, 353, 359, ...

# M500 Winter Weekend 2004

The twenty-third M500 Society WINTER WEEKEND will be held at **Nottingham University** from **Friday 2nd** to **Sunday 4th January 2004**.

This is an annual residential weekend to dispel the withdrawal symptoms due to courses finishing in October and not starting again until February. It's an excellent opportunity to get together with acquaintances, new and old, and do some interesting mathematics in a leisurely and friendly atmosphere. The event is run by Ian Harrison and this year's theme will be *The Geometry of Space and Time*. It promises to be as much fun as always!

Cost: £165 for M500 members, £170 for non-members. This includes accommodation and all meals from dinner on Friday to lunch on Sunday. Please send a stamped, addressed envelope for a booking form to

**Norma Rosier**

Enquiries by e-mail to Norma@M500.org.uk.

# Contents M500 194 – October 2003

**Some maths from long ago**
Bob Escolme . . . . . 1

**Problem 194.1 – Normals to an ellipse** . . . . . 7

**Problem 194.2 – Surface area of an ellipsoid** . . . . . 7

**Solution 191.1 – Bee**
David Kerr . . . . . 8

**Solution 189.6 – Three friends**
Geoff Corris . . . . . 10

**Solution 191.7 – Sum and reciprocal**
David Kerr . . . . . 10
John Spencer . . . . . 11
John Bull . . . . . 12
Mike Lewis . . . . . 12

**Solution 191.6 – Porthole**
John Spencer . . . . . 14
David Singmaster . . . . . 16

**One-edge connections**
Ted Gore . . . . . 17

**A method of solving Vigenere ciphers**
Dick Boardman . . . . . 20

**Forty**
Eddie Kent . . . . . 21

**Prime primes**
Eddie Kent . . . . . 21

**Solution 191.9 – Switch**
Dick Boardman . . . . . 22

**Goat**
John Spencer . . . . . 23

**Solution 190.5 – Eight switches**
Dick Boardman . . . . . 24

**Letters to the Editors**
Proverbs Ralph Hancock . . . . . 25
Fermat numbers Colin Davies . . . . . 26
All the sevens Patrick Lee . . . . . 27
Marks Ron Potkin . . . . . 28

**Problem 194.3 – Sixteen lamps** . . . . . 28

**Problem 194.4 – Getting dressed** . . . . . 28

**Problem 194.5 – Cube** . . . . . 29

**What's missing?** . . . . . 29

**M500 Winter Weekend 2004** . . . . . 29