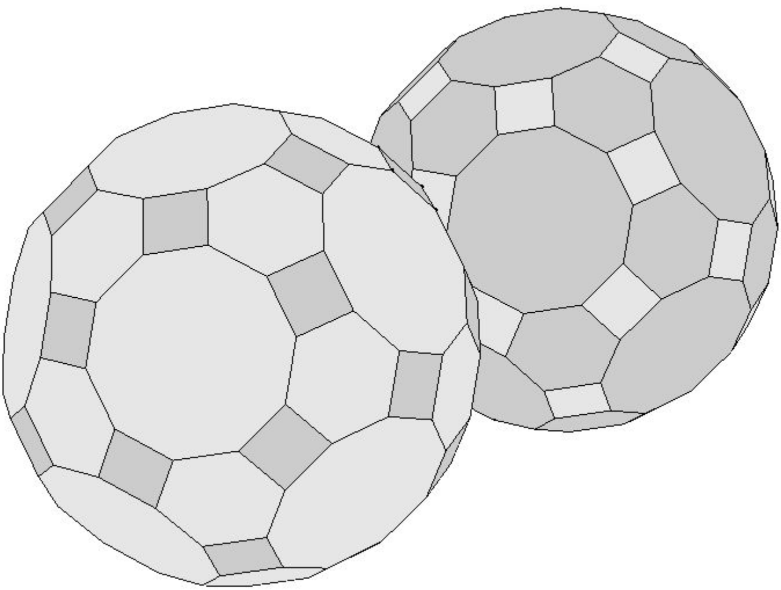
*

ISSN 1350-8539

M500 231



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 by organizing residential weekends, the Society aims to promote a better understanding of mathematics, its applications and its teaching. Web address: www.m500.org.uk.

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.

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

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. For details, send a stamped, addressed envelope to Diana Maxwell, 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 to tony@m500.org.uk.

The class number of certain quadratic fields

Tommy Moorhouse

Introduction Paul Jackson's article in M500 **225** indicated a connection between Wilson's theorem and the class number of a related field. While these terms might be unfamiliar it is interesting to look at where some of Paul's formulae might come from and what they mean. It is not possible to give even a brief overview of the subject of ideal class theory here, but we will work in such a way that no knowledge of this theory is required. The interested reader is referred to [Alaca & Williams] and [Stewart & Tall] for an introduction to algebraic number theory.

Along the way we will prove an interesting result about the parity of class numbers h of certain fields, for which no knowledge of ideal class groups is required, just a formula found by Dirichlet. For the sake of brevity we will not consider the special case $p = 3$.

Dirichlet's formula Dirichlet found a remarkable formula for the class number of a quadratic number field. A quadratic number field is an extension of $\mathbb{Q}$ by a root of a quadratic equation such as $x^2 + 7 = 0$. In this case we write $K = \mathbb{Q}(\sqrt{-7})$ and we can think of K as the smallest field containing $\mathbb{Q}$ and a square root of -7.

Dirichlet's formula for $K = \mathbb{Q}(\sqrt{-p})$, where p is prime, is

$$h(K) \;=\; \frac{-1}{p} \sum_{r=1}^{p-1} r(-p|r).$$

Here $(-p|r)$ is the quadratic residue symbol modulo r (or if $r = 2$ the Kronecker symbol – see [Alaca & Williams]). We can apply Dirichlet's formula to get an interesting result.

Theorem 1 *If p is an odd prime and $K = \mathbb{Q}(\sqrt{-p})$ then*

$$h(K) \;\equiv\; 1 \pmod 2 \qquad \text{if } p \equiv 3 \pmod 4$$

and

$$h(K) \;\equiv\; 0 \pmod 2 \qquad \text{if } p \equiv 1 \pmod 4.$$

Proof We reduce Dirichlet's formula modulo 2, multiplying both sides by $-p$ since $(p, 2) = 1$. This gives, reducing all the coefficients r modulo 2 and using $p \equiv 1 \pmod 2$,

$$h(K) \equiv \sum_{r=1,\, r=2k+1}^{p-1} (-p|r) \pmod 2.$$

Since $(p, r) = 1$ for all $r < p$ and $-1 \equiv 1 \pmod 2$, the sum simply counts, modulo 2, the number of positive odd integers less than p. If $p \equiv 3 \pmod 4$ this number is odd, while if $p \equiv 1 \pmod 4$ the sum is even. This proves the theorem.

Challenge Can you apply this method when $K = \mathbb{Q}(\sqrt{-n})$ where n is composite?

Paul Jackson quoted a formula given by Kenneth Ribet. It is possible to derive this formula directly using Dirichlet's formula. We want to find the sum of the quadratic residues modulo a prime of the form $p \equiv 3 \pmod 4$. It is easy to show that the sum is congruent to zero modulo p, but we want the actual value, which we denote by mp. We have

$$\begin{aligned} mp &= \sum_{(r|p)=1} r \\ &= \frac{1}{2}\sum_r r\{(r|p) + 1\} \\ &= \frac{1}{2}\sum_r r(r|p) + \frac{1}{4}p(p-1), \end{aligned}$$

where the second line picks out the quadratic residues. The sum in the last line is very reminiscent of Dirichlet's formula, and we will see that this is not a coincidence.

We will need to use the quadratic reciprocity law and the formulae for $(-1|r)$ and $(2|r)$ (see [Apostol, Chapter 9]).

First, take the case $r \equiv 1 \pmod 4$. Then

$$(-p|r) = (-1|r)(p|r) = (-1)^{(r-1)/2}(r|p) = (r|p).$$

If $r \equiv 3 \pmod 4$ we have

$$(-p|r) = (-1|r)(p|r) = (-1)^{(r-1)/2}(-(r|p)) = (r|p).$$

Thus $(-p|r) = (r|p)$ when r is odd.

To handle the case of even r we need to use the results from [Alaca & Williams, p. 246]. Since $p \equiv 3 \pmod 4$ we need to consider two cases.

Case 1: $p \equiv 3 \pmod 8$, in which case $-p \equiv 5 \pmod 8$ and $(-p|2) = -1$ while $(2|p) = (-1)^{(p^2-1)/8} = -1$.

Case 2: $p \equiv 7 \pmod 8$. Now $-p \equiv 1 \pmod 8$ and $(-p|2) = 1$ while $(2|p) = 1$.

Thus, by the multiplicative properties of the quadratic residue symbol, $(p|r) = (r|p)$ when r is even, too. In summary

$$\begin{aligned} m &= \frac{1}{2p}\sum_r r(-p|r) + \frac{1}{4}(p-1) \\ &= \{-2h(K) + p - 1\}/4, \end{aligned}$$

which is just the formula quoted by Paul. As a byproduct we have the alternative formula for the class number of $\mathbb{Q}(\sqrt{-p})$ for $p > 3, p \equiv 3 \pmod 4$):

$$h(K) = \frac{-1}{p}\sum_{r=1}^{p-1} r(r|p).$$

Challenge Can you extend this result to the case $p \equiv 1 \pmod 4$?

References

T. Apostol, *Introduction to Analytic Number Theory* (5th printing), Springer 1998.

S. Alaca and K. S. Williams, *Introductory Algebraic Number Theory*, Cambridge 2004.

I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem* (3rd ed.), A. K. Peters 2002.

Problem 231.1 – Log 12

Let $S_r = \displaystyle\sum_{n=4,\ n \text{ composite}}^{\infty} \frac{1}{n^r}$. Show that

$$\log 12 = 2\log\pi + S_2 + \frac{S_4}{2} + \frac{S_6}{3} + \frac{S_8}{4} + \cdots.$$

The Pell number 5

Non-trivially 5 is the only odd Pell number one more than a perfect square

Paul David Jackson

We show that non-trivially 5 is the only odd Pell number of the form X^2+1, where all odd Pell numbers are the sums of two squares. Also we see that 5 is the only odd Pell prime of this form.

Let $C_i = p_i/q_i$ be convergents to $\sqrt{2}$, the first few being

$$\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \frac{239}{169}, \frac{577}{408}, \frac{1379}{985}, \ldots;$$

then the q_i, or the denominators, are Pell numbers. By observation, the first few seem to obey the rule, that the squares of any two consecutive ones sum to another number in the sequence. So for instance we have $1^2 + 2^2 = 5$, $2^2 + 5^2 = 29$, $5^2 + 12^2 = 169$ and so on, with the sums 5, 29, and 169, all having odd indices. In fact we have the relation

$$q_{2k+1} \;=\; q_k^2 + q_{k+1}^2, \qquad k = 1, 2, 3, \ldots,$$

which can be proved using the standard identity $P_{m+n} = P_m P_{n+1} + P_{m-1}P_n$, valid for Pell numbers (see *Mathworld*, Pell Number, equation 6), by putting $m = k+1$, $n = k$ and swapping labels q, for P.

Now the odd indexed Pell numbers are all sums of two squares with opposite parities and thus are odd. This is obvious, and can be seen by considering the recurrence relation and the initial terms, being odd then even; so the next term is twice an even term plus an odd, hence odd, and then the next is twice an odd plus an even, hence even, and so on. Hence if q_{2k+1} is prime and greater than 5, or the square of a prime, then it is the sum of two squares in only one way, and as 1 occurs only once at the beginning of the sequence of the denominators of the convergents to $\sqrt{2}$, we see that these cannot be of the form X^2+1. This leaves the case where q_{2k+1} is not of the same form as above. That is, when it is composite. Rather than trying to factor these in some manner we consider another identity,

$$q_{2k+1} \;=\; 2p_k q_{k+1} - (-1)^k, \qquad k = 1, 2, 3, \ldots,$$

which can be proved using the standard identity $U_{2n+1} = U_{n+1}V_n - Q^n$, valid for the Lucas sequence (see *Mathworld*, Lucas sequence, equation 47), with $U_n(P,Q) = U_n(2,-1)$, and $V_n(P,Q) = V_n(2,-1)$. Then we set $U_n = q_k$, and $V_n = 2p_k$.

So if there are any odd Pell numbers after 5 of the form a square plus one then we would have $q_{2k+1} - 1 = z^2$, and this implies we have $2p_k q_{k+1} - (-1)^k - 1$ a square. Now if k is odd we have $2p_k q_{k+1} = z^2$ (which is true for 5) and if k is even we have $2p_k q_{k+1} - 2 = 2(p_k q_{k+1} - 1) = 2p_{k+1} q_k = z^2$ using the standard identity

$$p_k q_{k+1} - p_{k+1} q_k = (-1)^k. \qquad \text{(i)}$$

In both cases we have supposed squares of the form $2ab$, we show below that the two factors a, and b are co-prime, so to have squares we would need $a = 1$, and $b = 2$, the case for 5, or in general, as the as are odd, a a square, and b twice a square. We show in general this is impossible.

Assume to the contrary that we have, $b = 2b'$ where b' is a square. We know that there are no cases for the first few convergents so this means we can take $b' > 1$. Now for both possibilities of k, q_i is an even Pell number, so we need to exclude the possibility that it is twice a square. As it is even this means the index is even and for all even Pells we have the relation

$$q_{2s} = 2p_s q_s, \qquad s = 1, 2, 3, \ldots .$$

Now if s is even then p_s has the form square + 1 and so cannot be a square. Thus even if q_s, is twice a square, as p_s, and q_s, are co-prime, twice their product cannot be a square, as of course neither is unity.

Lastly, say s is odd then q_{2s} cannot be twice a square as both p_s, and q_s are co-prime again and all of the odd indexed $q_i > 1$ are not squares except for 169 (Wells, page 133), which as its associated numerator 239 is not a square does not lead to a q_{2s}, being twice a square. So we see in general that q_{2s} is not twice a square.

Therefore we see that our supposed squares $q_{2k+1} - 1 = z^2$ cannot exist. So to complete the argument we show that in general the pairs of numbers (p_k, q_{k+1}) and (p_{k+1}, q_k) are co-prime.

The convergents to $\sqrt{2}$ are in their lowest terms and satisfy the standard relation (i). This has the form $mx + ny = 1$, implying that the two terms of (i) on the LHS share no common factors with each other but not that the pairs of numbers p_k, q_{k+1} and p_k, q_{k+1} are themselves co-prime, which is what we want. But if we consider the consecutive convergents as rational numbers to which we add an integer c, we obtain $p_i/q_i + c = (p_i + cq_i)/q_i$. That is if we write (i) in the form

$$\frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}} = \frac{(-1)^k}{q_{k+1} q_k}$$

and then if we add zero $= c - c$ to the LHS, we get

$$\frac{p_k}{q_k} + c - \frac{p_{k+1}}{q_{k+1}} - c \;=\; \frac{p_k + cq_k}{q_k} - \frac{p_{k+1} + cq_{k+1}}{q_{k+1}} - c \;=\; \frac{(-1)^k}{q_{k+1}q_k},$$

which shows that the new convergents formed by adding a constant are also co-prime.

This is a general argument that will apply to any convergents to an irrational, but we have to relate it to the convergents to $\sqrt{2}$. We show that the new numerators obtained by the addition of a constant are just the numerators of the convergents to $\sqrt{2}$, but shifted relative to the denominators.

Now if k is odd we obtain the sequence of rationals (including the even indexed values as well)

$$\frac{1}{2},\ \frac{3}{5},\ \frac{7}{12},\ \ldots, \qquad \text{sequence A}$$

and if k is even we obtain the sequence of rationals (including the odd indexed values)

$$\frac{3}{1},\ \frac{7}{2},\ \frac{17}{5},\ \ldots. \qquad \text{sequence B}$$

Both of these are just the original convergents to $\sqrt{2}$, but with numerators and denominators of the original terms shifted against each other, thus they satisfy the same linear recurrence equations but with different initial terms, which are still just the terms in the original numerators and denominators to $\sqrt{2}$. Thus their continued fraction representations will have the same repeated part, $[a, b, \ldots, \langle 2 \rangle]$.

If we invert each term in sequence A the property of being co-prime is unaffected and we observe that the new sequence we obtain,

$$\frac{1}{2},\ \frac{5}{3},\ \frac{12}{7},\ \ldots, \qquad \text{sequence A}'$$

can be got from the convergents to $\sqrt{2}$, by inverting then adding 1 to each. We suspect that sequence A$'$ converges to $1 + 1/\sqrt{2}$, and taking this irrational number and using the continued fraction algorithm we obtain the representation $[1, 1, \langle 2 \rangle]$ for which we generate the convergents in the normal manner, and we find that after the third, we have numerators and denominators of the form $r_{k+1} = 2r_k + r_{k-1}$, and we must get the same sequences for these as we do for the continued fraction of $\sqrt{2}$ but shifted appropriately relative to each other, as we do for sequence A$'$. Thus sequence A$'$ is generated by $[1, 1, \langle 2 \rangle]$, and does represent $1 + 1/\sqrt{2}$.

For sequence B we have a similar situation; this converges to $2+\sqrt{2} = [3, \langle 2\rangle]$. We have the same linear recurrence relation for numerators and denominators as for $\sqrt{2}$ but with initial terms $p_1 = 3$, $p_2 = 7$, and $q_1 = 1$, $q_2 = 2$, so we will get the same sequences of numerators and denominators as for convergents to $\sqrt{2}$ but shifted. We can obtain sequence B from the convergents to $\sqrt{2}$ but this time by adding 2 to each. And we note in passing that in general the continued fraction of $c+\sqrt{2}$ with c a non-negative integer, is $[c+1, \langle 2\rangle]$. In short as the convergents generated by the continued fraction of an irrational have co-prime numerators and denominators, we have shown that the continued fraction of $1 + 1/\sqrt{2}$ generates sequence A′, which implies that pairs of numbers p_k, q_{k+1} are co-prime, and likewise the continued fraction of $2+\sqrt{2}$ generates sequence B which implies that p_{k+1}, q_k are co-prime. So we have shown that in general the pairs of numbers p_k, q_{k+1} and p_{k+1}, q_k are co-prime, and that non-trivially 5 is the only odd Pell number of the form $X^2 + 1$, where all odd Pell numbers are sums of two squares.

References

http://mathworld.wolfram.com/PellNumber.html.

http://mathworld.wolfram.com/LucasSequence.html.

http://mathworld.wolfram.com/ContinuedFraction.html.

David Wells, *Curious and Interesting Numbers*, Penguin 1997.

Problem 231.2 – 45 degrees

Show that

$$\frac{\pi}{4} = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{2n-1}\left(\frac{6}{9^n} + \frac{7}{49^n}\right) = \frac{17}{21} - \frac{713}{27783} + \frac{33857}{20420505} - \cdots.$$

Problem 231.3 – No survivors

There are n people in a room. At each tick of the clock each person shoots (dead) another person chosen at random. The game stops when the number of players is reduced to 0 or 1. What's the probability of no survivors?

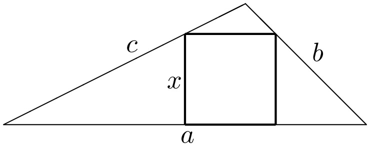
I couldn't resist taking a whack. The bat cracked and the ball shot straight over the pitcher's head, still picking up speed and altitude.

— *Four Blind Mice* by James Patterson [sent by Jeremy Humphries]

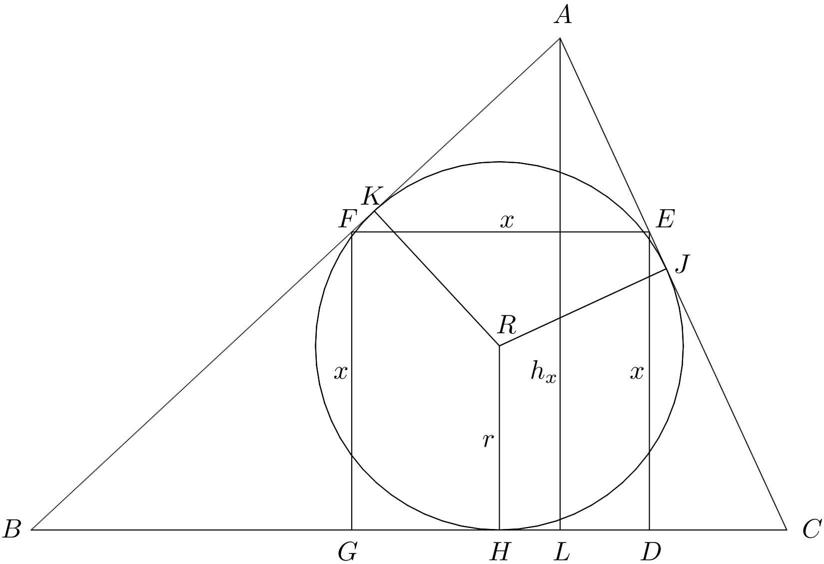
Solution 226.4 – Three squares

Let $\mathcal{T}$ be a triangle with sides a, b, c and in-circle radius r. Let x be the side of the square such that (i) one side of the square shares a common border with side a of $\mathcal{T}$, (ii) the other two vertices of the square lies on sides b and c of $\mathcal{T}$. Define y and z similarly in terms of sides b and c respectively. Show that

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z} = \frac{1}{a}+\frac{1}{b}+\frac{1}{c}+\frac{1}{r}.$$



Steve Moon



Let the in-circle of $\triangle ABC$ have centre R, radius r and be tangential to BC at H, CA at J and AB at K. Let the corners of the square as defined by side x be D, E, F and G. Let h_x be the perpendicular from side BC to vertex A, meeting BC at L. Then y and z are defined by cycling $a \to b \to c \to a$ once and twice respectively. Using the above diagram, points H, J, K and R are fixed in all three cases. Points corresponding to D, E, F and G will differ for y and for z. In general, $h_x \neq h_y \neq h_z$.

Now $\triangle ABC$ and $\triangle AFE$ are similar (since $EF||BC$). Hence

$$\frac{x}{AF} = \frac{a}{c}; \qquad AF = \frac{cx}{a}.$$

Also $\triangle FBG$ and $\triangle ABL$ are similar ($FG||AL$). Hence

$$\frac{x}{BF} = \frac{h_x}{c}; \qquad BF = \frac{cx}{h_x}.$$

Since $AF + BF = c$, we have $cx/a + cx/h_x = c$. Therefore

$$\frac{1}{x} = \frac{1}{a} + \frac{1}{h_x}. \tag{1}$$

If we repeat this for y and z, we get

$$\frac{1}{y} = \frac{1}{b} + \frac{1}{h_y}, \qquad \frac{1}{z} = \frac{1}{c} + \frac{1}{h_z}. \tag{2}$$

Adding (1) and (2) generates

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \left(\frac{1}{h_x} + \frac{1}{h_y} + \frac{1}{h_z}\right).$$

Returning to the diagram, the area of $\triangle ABC$ is $\frac{1}{2}ah_x$. Also we can make $\triangle ABC$ from $\triangle ARB$, $\triangle ARC$ and $\triangle BRC$, where, in turn, c, b and a are the bases and r the vertical height. Hence we have another expression for the area of $\triangle ABC$:

$$\frac{ar}{2} + \frac{br}{2} + \frac{cr}{2} = \frac{1}{2}ah_x.$$

Therefore

$$h_x = \frac{(a+b+c)r}{a}; \qquad \frac{1}{h_x} = \frac{a}{(a+b+c)r}.$$

Similarly for y and z we get $\dfrac{1}{h_y} = \dfrac{b}{(a+b+c)r}$ and $\dfrac{1}{h_z} = \dfrac{c}{(a+b+c)r}$. Therefore

$$\frac{1}{h_x} + \frac{1}{h_y} + \frac{1}{h_z} = \frac{a}{(a+b+c)r} + \frac{b}{(a+b+c)r} + \frac{c}{(a+b+c)r} = \frac{1}{r}.$$

Hence

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{r},$$

as required.

Unrest on Tetra

Tommy Moorhouse

There is unrest on the planet Tetra. Tetra is a tetrahedral world, where the inhabitants are confined to the two-dimensional surface. The inhabitants have for many years intercepted television signals from Earth and have become fascinated by old OU physics programmes. Inspired by the ideas of general relativity, one great scientist and adventurer, Hingis the Insatiable, has sought to prove that Tetra has curvature. He organized an expedition around the planet on a path (path A of Figure 1), encircling one of the four poles (the vertices of the tetrahedron). At the start of the expedition an arrow was marked on the planet's surface at an angle of θ to the path. A second arrow was set to this angle and taken along on the expedition. At all times during the expedition the movable arrow was kept at the same angle, measured as follows.

Imagine that lines are drawn on the first of Tetra's faces to be traversed, parallel to the starting edge (Figure 2). The angle between the moving arrow and the lines was kept constant as long as the expedition was on this face. When an edge was encountered the imaginary lines were continued to the next face by the method of Figure 3. That is, the tetrahedron was imagined to be 'flattened out' without distorting the surface, the imaginary lines were continued to the next face, and the tetrahedron folded up again. The arrow was always kept at the same angle to the extended lines. When, after months of toil, the expedition returned to the starting point, the movable arrow was compared to the marked arrow and it was found that they made different angles with the path. In fact, the arrows now pointed in opposite directions, a change of π radians.

Hingis deduced that, since the change in the angle is a measure of the curvature enclosed by the path, Tetra has a total curvature of 4π, the same as a sphere.

Hingis's findings have enraged his rival Grubor the Excitable. Grubor is an advocate of the 'Flat Tetra' theory. His rival expedition took path B, marking an arrow on the surface and taking one on the expedition as with Hingis' expedition. Back at the starting point over a year later the angle between the two arrows was zero. Grubor says this proves the 'Flat Tetra' theory and that Hingis is a fraud. Hingis is unimpressed by this slur on his integrity.

Civil war is imminent. Who is right? Is there any possibility of reconciliation of the results?

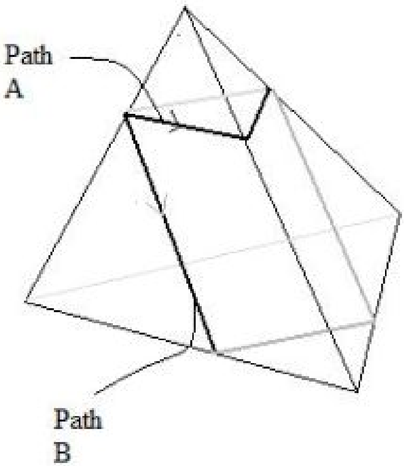


Figure 1

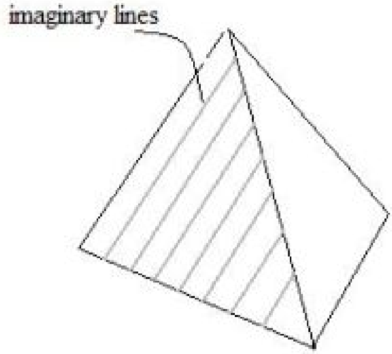


Figure 2

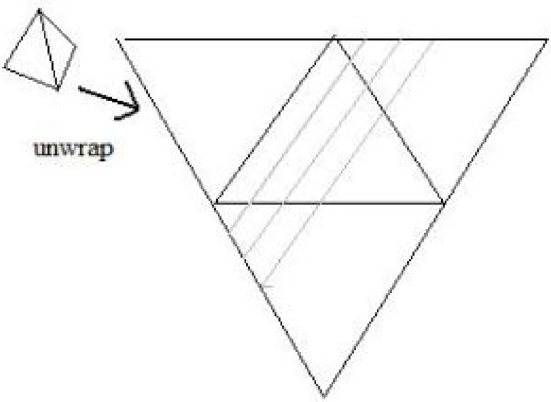


Figure 3

Where Mathematics Comes From

George Lakoff & Rafael Núñez,
Basic Books, 2000

Sebastian Hayes

So where does it come from according to these authors? The answer seems to be: '... [from] concepts in our minds that are shaped by our bodies and brains and realized physically in our neural systems' (p. 346). One might consider this a rather obvious, not to say bland, conclusion but it is not a theory the mathematical establishment is going to accept any day soon. Why not? Because it knocks out the 'transcendental origin' theory, otherwise known as Platonism, to which practically all professional mathematicians subscribe either openly or covertly. The authors point out that there is no way such a claim could be tested, so it cannot really be considered a scientific hypothesis.

The authors demonstrate fairly convincingly that many of the sophisticated mathematical procedures we employ can be traced back to primitive schemas, such as the 'Container Schema' which underlies Set Theory and Boolean Logic, schemas which are themselves abstractions from physical sensations made by—wait for it—infants in arms. 'Mathematics ... is grounded in the human body and brain, in human cognitive capacities, and in common human activities and concerns' (p. 358).

All this is, of course, not news to me since I have, off and on, been advancing some such theory of the origin of mathematics in these pages for the last thirty years, but it is nice to see some of the details of these familiar cognitive 'grounding metaphors' fleshed out. The dreadful fact is that mathematicians, pure just as much as applied, cannot get on without metaphors culled from sensory experience, and, far from 'transcending' these metaphors by abstraction, all too often mathematicians remain pathetically tied to these conceptions, the 'metaphor' of the Number Line being the most grotesque example. For, whatever numbers 'really' are, they certainly are not points on a line and they are not at a specific distance from a mathematical 'origin'.

From my point of view, the book does not go far enough, since it (just) stops short of developing a truly empirical theory of mathematics, largely because of the excessive importance the authors give to what they call the *Basic Metaphor of Infinity* (BMI)—for if there is one mathematical concept that is not grounded in our sensory experience (except in a strictly privative sense), it is infinity.

Also, the book is too long—nearly 500 large pages—though anything shorter would have been dismissed by the establishment as superficial. For all that, this is a very welcome book and a brave one too, since the authors remark at one point, with commendable understatement, that 'it is not unusual for people to get angry when told that their unconscious conceptual systems contradict their fondly held conscious beliefs' (p. 339). Out of context, you might think Lakoff & Núñez were referring to hardline Creationists from the Bible Belt in America—but no, 'people' in this quote simply means professional mathematicians.

Solution 228.3 – Another arithmetic progression

> The three sides of a triangle are in arithmetic progression with common difference 1. The largest angle exceeds the smallest by 90°. What are the sides?

Brian Howlett

Define the triangle as having sides $a-1$, a and $a+1$ and smallest angle A. Then the largest angle is $A+90^\circ$ and the third angle is $90^\circ - 2A$.

Now use the cosine rule in the form $\cos A = \dfrac{b^2+c^2-a^2}{2bc}$, using the usual notation. So for the smallest angle we have

$$\cos A \;=\; \frac{a^2+(a+1)^2-(a-1)^2}{2a(a+1)} \;=\; \frac{a+4}{2(a+1)}.$$

For the third angle, since $\cos(90^\circ + A) = -\sin A$, the cosine rule gives

$$-\sin A \;=\; \frac{a^2+(a-1)^2-(a+1)^2}{2a(a-1)} \;=\; \frac{a-4}{2(a-1)}.$$

Now, making use of the well-known formula $\sin^2\alpha + \cos^2\alpha = 1$, we have

$$\left(\frac{a-4}{2(a-1)}\right)^2 + \left(\frac{a+4}{2(a+1)}\right)^2 \;=\; 1.$$

Algebraic manipulation, left as an exercise for the reader, reduces this to $a^4 - 5a^2 - 14 = 0$. So $(a^2+2)(a^2-7) = 0$. Of the four solutions, only $a = \sqrt{7}$ satisfies the triangle problem. Hence the required triangle has sides $\sqrt{7}-1$, $\sqrt{7}$ and $\sqrt{7}+1$.

Also solved by **Sebastian Hayes**, **Steve Moon** and **Norman Graham**.

Two Millennia of Mathematics: From Archimedes to Gauss

George M. Phillips,
Canadian Mathematical Society, Springer, 2000.

Eddie Kent

'In an ideal university the staff would supplement the standard courses by offering lectures in which they talked about topics which they particularly loved ... ' begins a review of this book in the LMS Newsletter. No doubt; but of course attending these lectures wouldn't propel you through any exam. For that you need something like the M500 Weekend. However, once over that hump this book is fun to read.

Professor Phillips's supervisor at Aberdeen was Edward Wright, of Hardy & Wright *An Introduction to the Theory of Numbers* and of Aberdeen's Sir Edward Wright Building. Apart from a few years at Southampton he stayed for most of his career at St Andrews University. He wears a Mackenzie tartan tie and speaks Doric, a language that is not difficult to read once you grasp that, for instance, 'Tatatitore' means 'Goodbye to Torry'.

As a preliminary, George enters the debate over whether results in mathematics are created or discovered. He compares Bach, Shakespeare and Gauss, all figures of comparable status in their fields, and points out that of the three only the work of Gauss does not retain his individual identity. All his achievements would sooner or later have been discovered by someone else. This book then is an account of those discoveries that have interested the author in particular, and of how they came about. Often, he maintains, found by ordinary mortals. (Oh, to be so ordinary.)

The chapters are (1) From Archimedes to Gauss [going from π to the AGM], (2) Logarithms, (3) Interpolation, (4) Continued fractions [Fibonacci pops up here], and (5) More number theory [travelling from primes to sums of cubes, and including the story of F. N. Cole who at a meeting of the American Mathematical Society in 1903, without saying a word, multiplied 193707721 by 761838257287 to show that the product is the 67th Mersenne number]. Each chapter gives the history of its subject, starting quite innocently but digging deeper into complexity and rigour until by a very few pages into the chapter you start to wish you were sitting comfortably with pencil and paper. All of the mathematics follows logically if sometimes a little unexpectedly, and there are many curious incidents and accidents that are a sheer delight to read. To enjoy this book you must love mathematics.

The book is excellently produced, as one would expect from Springer, with a bright shiny cover and acid-free pages. It has an index and a bibliography (containing 11 items by G. M. Phillips, an indication that the subjects are those close to George's heart); altogether coming to 223 pages. It follows the irritating custom of numbering each type of object separately, so you get section 2.1, equation 2.1, figure 2.1, etc., but I suppose some people like this and can handle it. Another irritation is that although the book is clearly aimed at people who can handle mathematics, it nevertheless feels obliged to point out that a useful table of logarithms would have more than five entries. But that is me wearing my editorial hat.

I make no pretence to judge the mathematics; in fact I had trouble enough following most of it (look how long I've taken), but I was cheered by the Samuel Johnson quotation – 'Sir, I have found you an argument; but I am not obliged to find you an understanding.' Sam can always be relied on. And so can George, who seeks to express sometimes difficult ideas with impressive simplicity.

Problem 231.4 – Four tans

Prove that

$$\tan 70^\circ \;=\; \tan 20^\circ + 2\tan 40^\circ + 4\tan 10^\circ.$$

Problem 231.5 – Four cos and four sins

Prove that

$$\frac{\cos^4 A}{\cos^2 B} + \frac{\sin^4 A}{\sin^2 B} \;=\; 1 \quad\Rightarrow\quad \frac{\cos^4 B}{\cos^2 A} + \frac{\sin^4 B}{\sin^2 A} \;=\; 1.$$

Problem 231.6 – Three arctans

Suppose $a, b, c > 0$. Prove that

$$\arctan\sqrt{\frac{a(a+b+c)}{bc}} + \arctan\sqrt{\frac{b(a+b+c)}{ca}} + \arctan\sqrt{\frac{c(a+b+c)}{ab}} \;=\; \pi.$$

What if there is no restriction on a, b and c?

Errors using inadequate data are much less than those using no data at all.

— Charles Babbage

Solution 227.7 – Pentagonal numbers

Let $\mathcal{P} = \{0, 1, 2, 5, 7, 12, 15, 22, 26, 35, 40, 51, 57, 70, 77, 92, \dots\}$ be the set of (generalized) pentagonal numbers, that is, integers of the form $(3r^2 \pm r)/2$, $r = 0, 1, 2, \dots$. Which arithmetical progressions avoid $\mathcal{P}$?

Steve Moon

For a range of (a, b), I had a look for patterns, with the following results for arithmetic progressions $at + b$, $t = 0, 1, 2, \dots$, $a > 0$, $0 \le b < a$.

a	b for which no member of $\mathcal{P}$ generated (for $at + b < 1000$)
1	–
2	–
3	–
4	–
5	3, 4
6	–
7	3, 4, 6
8	–
9	–
10	3, 4, 8, 9
11	3, 6, 8, 9, 10
12	–
13	3, 4, 6, 8, 10, 11
14	3, 4, 6, 10, 11, 13
15	3, 4, 8, 9, 13, 14
16	–
17	3, 4, 8, 10, 11, 13, 14, 16
18	–
19	4, 6, 8, 9, 10, 11, 14, 17, 18
20	3, 4, 8, 9, 13, 14, 18, 19
21	3, 4, 6, 10, 11, 13, 17, 18, 20
22	3, 6, 8, 9, 10, 14, 17, 19, 20, 21
23	4, 6, 9, 10, 13, 14, 16, 18, 19, 20, 21
24	–
25	3, 4, 6, 8, 9, 11, 13, 14, 16, 18, 19, 21, 23, 24
26	3, 4, 6, 8, 10, 11, 16, 17, 19, 21, 23, 24
27	–

Observations.

(a) No solutions for primes 2 and 3.

(b) No solutions for values of a of the form $2^m 3^n$, $m, n = 0, 1, 2, \ldots$.

(c) For a prime, $a = p$, $p \geq 5$, there are $(p-1)/2$ values of b.

(d) For a of the form $a = pk$, p prime, $p \geq 5$, k an integer, solutions can be generated by taking values of b which are solutions for $a = p$ and then adding p to each b, subject to generated values of b for $a = pk$ having $b < a$; e.g.

$$\begin{array}{lllllll} a = 5 & \longrightarrow & b = 3,\ 4; & & & & \\ a = 10 & \longrightarrow & b = 3,\ 4 & \stackrel{+5}{\longrightarrow} & 8,\ 9; & & \\ a = 15 & \longrightarrow & b = 3,\ 4 & \stackrel{+5}{\longrightarrow} & 8,\ 9 & \stackrel{+5}{\longrightarrow} & 13,\ 14. \end{array}$$

So, if we can generate values of b which cause the arithmetic progression to avoid $\mathcal{P}$, we can generate solutions for any composite a not of the form $a = 2^m 3^n$.

It is easier to find the values of b which *do* generate members of $\mathcal{P}$ for prime $a \geq 5$; then the set we need is the complement, there being a total of p possible values of b, including 0.

For (a, b) generating $at + b \in \mathcal{P}$ for some t, we have

$$\frac{3r^2 \pm r}{2} \equiv b \pmod{a = p}, \qquad p \geq 5.$$

Since $\gcd(p, 2) = \gcd(p, 3) = 1$ and $24 = 2^3 \cdot 3$ we can multiply both sides of the congruence by 24 to obtain $36r^2 \pm 12r \equiv 24b \pmod{p}$ and complete the square to get

$$(6r \pm 1)^2 \equiv 24b + 1 \pmod{p}.$$

Now we need the quadratic residues of p. There are $(p-1)/2$, given by evaluating $1^2, 2^2, 3^2, \ldots, \left(\frac{1}{2}(p-1)\right)^2$ modulo p. If you continue beyond $\left(\frac{1}{2}(p-1)\right)^2$ to $(p-1)^2$, you get no new solutions; the numbers appear twice. We also need 0^2; so there will be $(p+1)/2$ quadratic residues. Hence, for $a = p$, there will be $p - (p+1)/2 = (p-1)/2$ values of b that generate $at + b$ avoiding $\mathcal{P}$.

We next proceed by finding the set of solutions to $24b + 1 \equiv s$, where s is a quadratic residue of b, or zero, and then the complement of this set is what we want. By way of example, take $a = 23$, the same as in the original statement of the problem.

$0^2 \equiv 0 \pmod{23}$	$\longrightarrow$	$24b \equiv 0$	$\longrightarrow$	$b = 22$
$1^2 \equiv 22 \equiv 1 \pmod{23}$	$\longrightarrow$	$24b \equiv 1$	$\longrightarrow$	$b = 0$
$2^2 \equiv 21 \equiv 4 \pmod{23}$	$\longrightarrow$	$24b \equiv 4$	$\longrightarrow$	$b = 3$
$3^2 \equiv 20 \equiv 9 \pmod{23}$	$\longrightarrow$	$24b \equiv 9$	$\longrightarrow$	$b = 8$
$4^2 \equiv 19 \equiv 16 \pmod{23}$	$\longrightarrow$	$24b \equiv 16$	$\longrightarrow$	$b = 15$
$5^2 \equiv 18 \equiv 2 \pmod{23}$	$\longrightarrow$	$24b \equiv 2$	$\longrightarrow$	$b = 1$
$6^2 \equiv 17 \equiv 13 \pmod{23}$	$\longrightarrow$	$24b \equiv 13$	$\longrightarrow$	$b = 12$
$7^2 \equiv 16 \equiv 3 \pmod{23}$	$\longrightarrow$	$24b \equiv 3$	$\longrightarrow$	$b = 2$
$8^2 \equiv 15 \equiv 18 \pmod{23}$	$\longrightarrow$	$24b \equiv 18$	$\longrightarrow$	$b = 17$
$9^2 \equiv 14 \equiv 12 \pmod{23}$	$\longrightarrow$	$24b \equiv 12$	$\longrightarrow$	$b = 11$
$10^2 \equiv 13 \equiv 8 \pmod{23}$	$\longrightarrow$	$24b \equiv 8$	$\longrightarrow$	$b = 7$
$11^2 \equiv 12 \equiv 6 \pmod{23}$	$\longrightarrow$	$24b \equiv 6$	$\longrightarrow$	$b = 5$

Hence, terms in $\mathcal{P}$ are generated by 0, 1, 2, 3, 5, 7, 8, 11, 12, 15, 17, 22, and $\mathcal{P}$ is avoided by $b =$ 4, 6, 9, 10, 13, 14, 16, 18, 19, 20, 21.

To show how to generate b for composite a, here is an example for $a = 35$, the smallest a which is the product of two distinct primes ≥ 5. Since $35 = 5 \cdot 7$, we can generate values of b from the results for $a = 5$ and $a = 7$.

$$a = 5 \rightarrow (3,4),\ (8,9),\ (13,14),\ (18,19),\ (23,24),\ (28,29),\ (33,34);$$
$$a = 7 \rightarrow (3,4,6),\ (10,11,13),\ (17,18,20),\ (24,25,27),\ (31,32,34).$$

Some results are duplicated, but we predict b not generating members of $\mathcal{P}$ for $a = 35$ with $b =$3, 4, 6, 8, 9, 10, 11, 13, 14, 17, 18, 19, 20, 23, 24, 25, 27, 28, 29, 31, 32, 33, 34. Hence we predict these values of b will generate members of $\mathcal{P}$: 0, 1, 2, 5, 7, 12, 15, 16, 21, 22, 26, 30. The quadratic residues of 35 are 1, 4, 9, 11, 14, 15, 16, 21, 25, 29, 30 plus 0.

$24b \equiv 0 \pmod{35}$	$\longrightarrow$	$b = 16$	$24b \equiv 15 \pmod{35}$	$\longrightarrow$	$b = 21$
$24b \equiv 1 \pmod{35}$	$\longrightarrow$	$b = 0$	$24b \equiv 16 \pmod{35}$	$\longrightarrow$	$b = 5$
$24b \equiv 4 \pmod{35}$	$\longrightarrow$	$b = 22$	$24b \equiv 21 \pmod{35}$	$\longrightarrow$	$b = 30$
$24b \equiv 9 \pmod{35}$	$\longrightarrow$	$b = 12$	$24b \equiv 25 \pmod{35}$	$\longrightarrow$	$b = 1$
$24b \equiv 11 \pmod{35}$	$\longrightarrow$	$b = 15$	$24b \equiv 29 \pmod{35}$	$\longrightarrow$	$b = 7$
$24b \equiv 14 \pmod{35}$	$\longrightarrow$	$b = 2$	$24b \equiv 30 \pmod{35}$	$\longrightarrow$	$b = 26$

If a is a composite of three or more primes, following the same method for each prime (and not worrying about duplicates), we can find all b that do and do not generate members of $\mathcal{P}$. This covers all a of the form $a = kp_1^{m_1}p_2^{m_2}p_3^{m_3}\ldots$, p_i prime ≥ 5, m_i a positive integer, k some integer of the form 2^m3^n, $m, n \geq 0$.

Turning to primes 2 and 3, we have the following:

(i) $\dfrac{3r^2 \pm r}{2} \equiv b \pmod{2}$ and b can be only 0 or 1, and $r = 0, 1$ respectively generate members of $\mathcal{P}$; hence no solutions.

(ii) $\dfrac{3r^2 \pm r}{2} \equiv b \pmod{3}$ and b can be only 0, 1 or 2, and $r = 0, 1$ generate members of $\mathcal{P}$ for each; so again no solutions.

Using the same method as before, given no solutions for $p = 2$ or 3, there will be no solutions for a of the form $2^m 3^n$, $m, n = 0, 1, \ldots$.

So, to summarize, these arithmetic progressions $at + b$ avoid $\mathcal{P}$:

(a) a prime, $a \geq 5$, $b < a$, where b is not a solution of $24b + 1 \equiv q \pmod{a}$, for q a quadratic residue of a;

(b) a of the form $a = kp_1^{m_1} p_2^{m_2} p_3^{m_3} \ldots$, p_i prime ≥ 5, m_i a positive integer, k some integer of the form $2^m 3^n$, $m, n \geq 0$.

Letters

Fromage frais

Dear Eddie,

I see that the Diagram prize for the oddest book title of the year has been won by *The 2009–2014 World Outlook for 60-milligram Containers of Fromage Frais*. You may notice something strange about this title, which moved me to make a comment on *The Bookseller* website when the shortlist was announced. Possibly no one else noticed, but luckily the people at the magazine picked it up. The news story on *Yahoo UK* reported: 'Philip Stone of *The Bookseller* noted that the winning book, while having a fascinating title, was out of the range of most people's pockets, costing $1140. "What does the future hold for these items? Well, given that fromage frais normally comes in 60-gram containers, not 60-milligram, one would assume that the world outlook for 0.06-gram containers of fromage frais is pretty bleak. But I'm not willing to pay £795 to find out," he said.' This mistake raises the prospect of other book titles containing errors of magnitude, such as *The 0.39 Steps*, *Two Leagues Under the Sea*, and *Around the World in* 10^{80} *Days*. To which my friend Mindaugas adds *The 1.001 Nights*.

Best wishes

Ralph Hancock

Arithmetic progressions

Dear Tony,

Many thanks for the latest issue of M500 (No. 228). I try to read M500 as soon as it arrives as to do otherwise means postponement *sine die*. (Ask anyone who is retired and over-committed!)

I like to attempt the problems and the two on page 16 seemed to be within my capabilities. Problem 228.3 [see page 13]—a triangle whose sides differ by 1? Well, $(1, 2, 3)$ is a bit flat—so that won't do; and I know $(3, 4, 5)$ has a right angle. With all further increases in side length the triangle tries to become increasingly nearer to an equilateral. So the answer must be $(2, 3, 4)$ (!). What? The sides are not necessarily positive integers? Oh—that is problem 228.2!

Never mind! Let the smallest side be $a - 1$ and the smallest angle be A. Then the other two angles are $90^\circ + A$ and $90^\circ - 2A$. ... [see page 13 for something similar to the omitted details] ... to calculate $A = 24.295^\circ$ approx., and the three sides of the triangle, $a - 1 = \sqrt{7} - 1 \approx 1.64575$, $a = \sqrt{7} \approx 3.64575$ and $a + 1 = \sqrt{7} + 1 \approx 4.64575$.

Problem 228.2 [Find all (finite) arithmetic progressions containing only positive integer terms that have the sum of the first three terms 51 and the sum of the last four terms 332] must be easier. The sum of the first three terms is 51. That is, $3a+3d = 51$. Therefore $a+d = 17$. The average of the last four terms is 83 and the common difference must be even. There are only seven possible differences to check, which leads to two progressions:

$$(d = 4)\ 13, 17, 21, \ldots, 77, 81, 85, 89$$

and

$$(d = 12)\ 5, 17, 29, \ldots, 65, 77, 89, 101.$$

Chris Pile

TF writes—Problem 228.2 turned out to be popular, with quite a long list of contributors generating solutions. **Martin Hansen**, **Brian Howlett**, **Sebastian Hayes**, **Basil Thompson** and **Steve Moon**, not to mention myself, all solved it in more or less the same manner. If you drop the positiveness condition, you get two more solutions, namely −27, 17, 61, 105, 149 and −115, 17, 149, 281. Bearing in mind the arbitrary nature of the parameters, 51 and 332, I am inclined to suspect that the problem had an origin in real life as part of a grander scheme.

Nuclear matters

Tony,

I first came across nuclear magnetic resonance in an OU chemistry course around 1976. It was used for detecting hydrogen, phosphorus, and other elements with odd mass numbers, or odd numbers of protons and neutrons. (As far as I remember.)

Later on, I heard about 'MRI scanning', and realized that this must really be based on NMR. But apparently nuclear things were dangerous, and Watford had even been declared to be 'a nuclear free zone'. Hence the term 'NMR scanning' was unacceptable.

I suggest that might be one reason why the technical details were not explored further in a public radio broadcast.

Colin Davies

Laces

Travelators have been in the news recently with the discovery—made in a non-mathematical way by measuring journey times—that they can be slower than walking. This was reported in the New Scientist. There is a summary at http://www.tgdaily.com/content/view/43265/181/.

Eddie Kent

Dear Eddie,

Re: Problem 227.5 – Laces [Your journey involves walking at your normal constant pace partly along fixed ground and partly along a moving travelator. Should you stop to tie your undone shoe-laces whilst on the travelator? The correct mathematical answer is of course yes [M500 **230** 7]; but . . .]. Surely only a complete nincompoop would get on to a travelator with untied shoe laces, an irresistible invitation to the machinery to engulf your feet first like Uday Hussein's plastic shredder.

Ralph Hancock

Problem 231.7 – Prime

Let q be a prime of the form $4k + 3$. Let $p = 2q + 1$ be prime. Suppose $2^q \equiv 1 \pmod{p}$.

Either prove that p is prime, or find a counter-example.

Contents — M500 231 – December 2009

The class number of certain quadratic fields
Tommy Moorhouse . . . 1
Problem 231.1 – Log 12 . . . 3
The Pell number 5
Paul David Jackson . . . 4
Problem 231.2 – 45 degrees . . . 7
Problem 231.3 – No survivors . . . 7
Solution 226.4 – Three squares
Steve Moon . . . 8
Unrest on Tetra
Tommy Moorhouse . . . 10
Where Mathematics Comes From
Sebastian Hayes . . . 12
Solution 228.3 – Another arithmetic progression
Brian Howlett . . . 13
Two Millennia of Mathematics
Eddie Kent . . . 14
Problem 231.4 – Four tans . . . 15
Problem 231.5 – Four cos and four sins . . . 15
Problem 231.6 – Three arctans . . . 15
Solution 227.7 – Pentagonal numbers
Steve Moon . . . 16
Letters
Fromage frais — Ralph Hancock . . . 19
Arithmetic progressions — Chris Pile . . . 20
Nuclear matters — Colin Davies . . . 21
Laces — Eddie Kent . . . 21
Ralph Hancock . . . 21
Problem 231.7 – Prime . . . 21