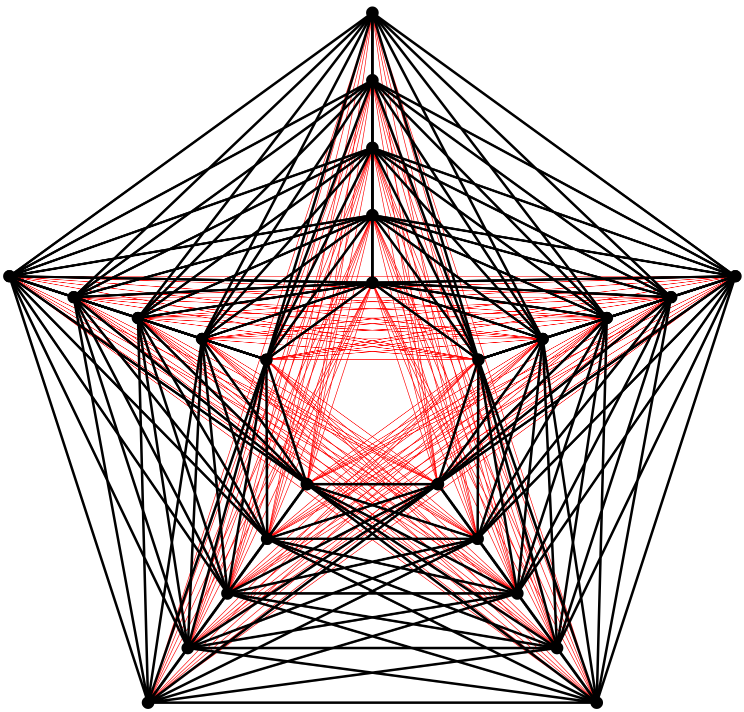
*

ISSN 1350-8539

M500 301



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: 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 Revision Weekend is a residential Friday to Sunday event providing revision and examination preparation for both undergraduate and postgraduate students. For details, please go to the Society's website.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. For details, please go to the Society's website.

Advice for 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 the Editor, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation. For more information, go to m500.org.uk/magazine/ from where a LaTeX template may be downloaded.

Christopher Pile

We regret to have to inform you that M500 Society member Christopher Pile died on 12 May 2021. Chris's connection with the Society goes back a long way, to the early years of the Open University. He was a great enthusiast for recreational mathematics, particularly anything to do with polyhedra. His first contributions to the M500 magazine appeared in 1976, and he has been a frequent contributor over the years since then.

Chinese sections

Alan Davies

1 Introduction

In the mid 1990s I went to a schools' lecture at the Royal Institution given by the late Pat Perkins. In the lecture she described the method of sections used by the ancient Chinese mathematicians to find the volumes of some common objects. I was particularly taken by the problem posed to find the volume common to two intersecting cylinders. I had, of course, seen the result using a triple integral in my undergraduate days. Since the principles involved are easily understood by year nine pupils, I developed a mathematics masterclass session to be presented in the series running at the University of Hertfordshire and I've presented it a number of times subsequently. Others have also done something similar. For readers interested in material suitable for presentation to a schools' audience the *Nrich* work produced by Emma McCaughan (2001) is an excellent resource.

2 Cavalieri's principle

Today we would recognise the method of these early Chinese mathematicians as the so-called Cavalieri's principle developed some thirteen hundred years later. In fact, this was not the first use of the technique. Archimedes, in the third century BC, had already developed a very similar method based on mechanical principles and he used it to find the volume of a sphere. The work, described in his *Method of mechanical theorems*, was thought to be lost but was found in the palimpsest (Wikipedia 2021a) discovered in 1906 (Heath 2002).

Bonaventura Cavalieri (1598 – 1647), as a disciple of Galileo, was encouraged to develop the idea of *indivisibles*, quantities which were infinitesimally small. In 1635 Cavalieri published the method in his highly-acclaimed *Geometria indivisibilus continuorum* and used it to develop the eponymous principle. We shall state his principle in the form given by Boyer (1968).

> *If two solids have equal altitudes and if sections made by planes parallel to the bases and at equal distances from them are always in the same ratio, then the volumes of the two solids are also in the same ratio.*

The principle is illustrated in Figure 1 where we have volumes V_1 and V_2 whose areas satisfy $A_1/A_2 = k$.

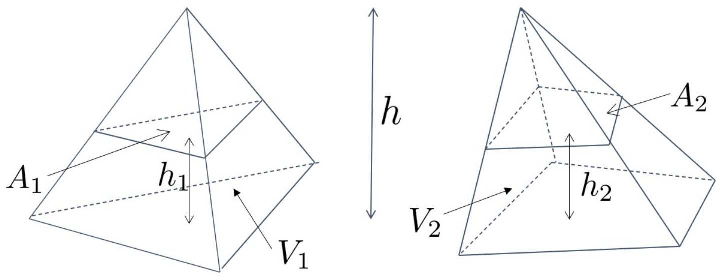


Figure 1: Solids with equal altitudes, h. Sections A_1 and A_2 in a constant ratio, k, when $h_1 = h_2$.

With $A_1/A_2 = k$, Cavalieri's principle states that $V_1/V_2 = k$. Cavalieri used his approach to deduce the volume of a sphere from the known volume of a cone and a cylinder (Wikipedia 2021b).

3 Chinese sections

We move back now to those early mathematicians in China and, in particular, to Liu Hui (*c*.225 – *c*.295) and his attempt to find a formula for the volume of a sphere. Liu Hui knew that a sphere of radius r could be circumscribed by a cube two of whose faces are horizontal and that the cube also circumscribes an object called a *móuhéfānggài* by the Chinese. The word móuhéfānggài literally means 'two close-fitted square lids'. The móuhéfānggài is the volume contained by the intersection of two horizontal cylinders, each of radius r, whose coplanar axes are perpendicular. It's also the volume contained by a pair of folding cloth mesh covers, the type used to protect food in the summer, see Figure 2, placed base-to-base.

Figure 2: Folding cloth mesh food cover.

The móuhéfānggài also circumscribes the sphere and the important property is that the cross sectional areas of the móuhéfānggài are squares which are in a constant ratio with the latitudinal small circles of the sphere. Hence if Liu Hui could find an expression for the volume of the móuhéfānggài he could find one for the volume of a sphere. Unfortunately for Liu Hui he was unable to find such an expression. It was another two hundred years before Zu Chongzhi (429 – 500) and his son Zu Gengzhi (*c*.450 – *c*.520) were able to find an expression for this much more complicated volume. Zu Chongzhi's major claim to mathematical fame is his amazingly accurate approximations to the value of π: $3.1415926 < \pi < 3.1415927$ and $\pi \approx 355/113$, the latter value not being known in Europe for another thousand years (Kiang 1972).

A note on Chinese names is worthwhile here. Zu Chongzhi is sometimes known as Tsu Ch'ung-Chih and it is in this form that a crater on the far side of the Moon is named. The word móuhéfānggài is written in the modern Hànyŭ Pīnyīn system now in use in China. The interested reader can find the Chinese symbols for the names in this article in the works of Kiang (1972), Lam and Shen (1985) and Polster (2004).

The yángmă

To follow the Chinese approach we first have to construct a *yángmă* (Brunton 1973). Every cube can be divided into three identical solids. Each of these solids is called a yángmă, see Figure 3. If the side of the cube is a then we shall say that the yángmă has side a.

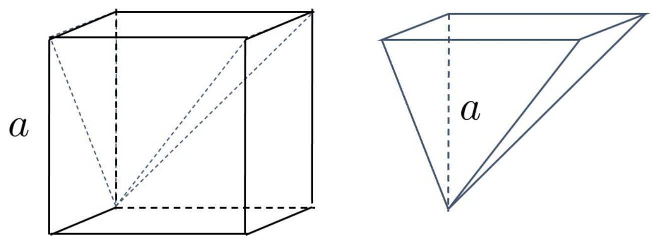


Figure 3: Yángmă, one third of a cube.

We shall need the value of the cross section of a yángmă, of side r, at a height x as shown in Figure 4.

Using similar triangles in Figure 4 we see that the cross section at height

x is a square of side x whose area is given by

$$A_{\text{yangma}} = x^2. \tag{1}$$

Since the cube has volume r^3 we can write

$$V_{\text{yangma}} = \frac{1}{3}r^3. \tag{2}$$

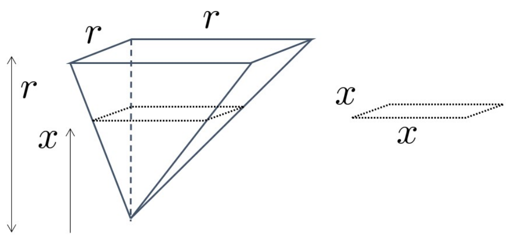


Figure 4: Cross section of yángmǎ at a height x.

In the Appendix the interested reader can find a template to make a yángmǎ from card.

The móuhéfānggài

Now, we turn our attention to the móuhéfānggài. Since it is the volume enclosed by the intersection of two identical cylinders, whose axes are orthogonal and lie in the same plane, the cross section in the plane of the axes is a square, see Figure 5.

If the cylinders have radius r then an octant of the móuhéfānggài fits snugly into a cube of side r, as shown in Figure 6(a).

The cross sections at height x are shown in Figure 6(b), where the dashes denote the square section of the cube, side r, and the solid lines form the square section of the móuhéfānggài whose side l is yet to be determined. A vertical section through the móuhéfānggài and the cube is shown in Figure 7 from which we see that

$$l^2 = r^2 - x^2.$$

Now the area of the L-shaped section in Figure 6(b) is given by

$$\begin{aligned} A_{\text{L-shape}} &= r(r-l) + l(r-l) \\ &= r^2 - l^2 = x^2 = A_{\text{yangma}}, \end{aligned}$$

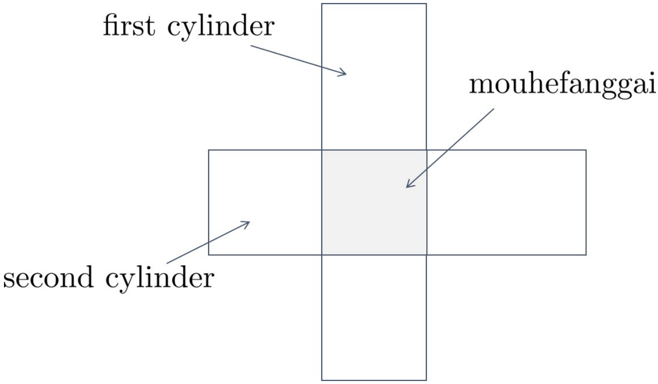


Figure 5: Intersection of two identical cylinders.

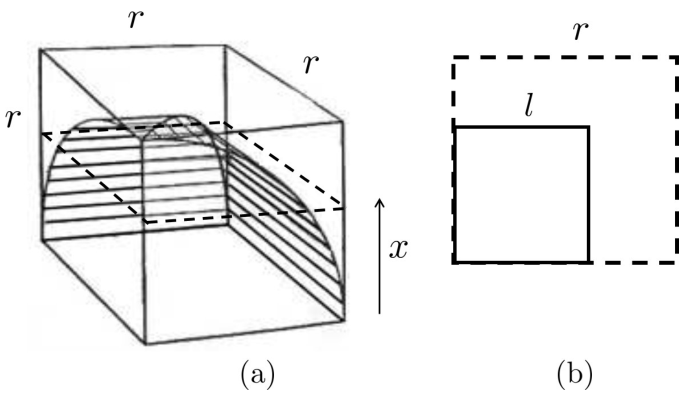


Figure 6: Octant of móuhéfānggài fitting snugly in a cube (after McCaughan, 2001).

using equation (1). Hence it follows, from equation (2) that

$$\begin{aligned} V_{\text{L-shape}} &= V_{\text{yangma}} \\ &= \frac{1}{3}r^3. \end{aligned}$$

If we consider the diagram in Figure 6 we see that the volume of the octant of the móuhéfānggài is given by

$$r^3 - V_{\text{L-shape}} = \frac{2}{3}r^3$$

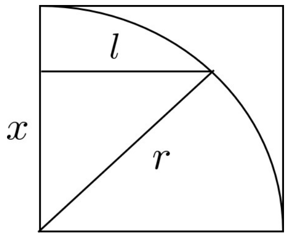


Figure 7: Vertical section through the móuhéfānggài and the cube.

and so

$$V_{\text{mouhefanggai}} = \frac{16}{3}r^3. \tag{3}$$

This was the value found by the Zus, father and son, in the fifth century. For completeness we shall show how they then used Liu Hui's idea to find the volume of a sphere.

The sphere

Now imagine a sphere of radius r fitting snugly inside the móuhéfānggài. A horizontal slice at height x is shown in Figure 8(a).

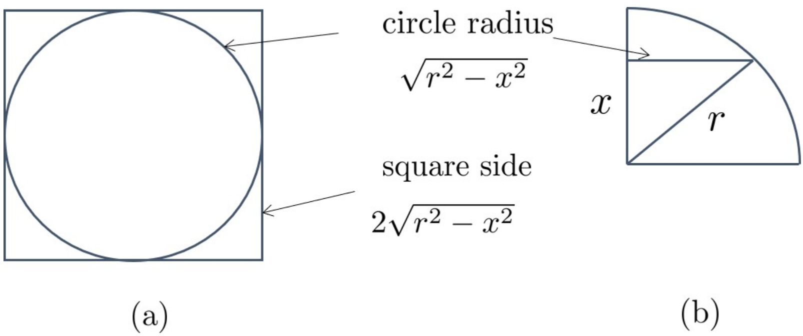


Figure 8: (a) Horizontal slice at height x, (b) vertical section through the octant of the sphere.

In Figure 8(b) we show a vertical slice through an octant of the sphere and from the diagrams in Figure 8 we see that

$$A_{\text{circle}} = \pi(r^2 - x^2) \quad \text{and} \quad A_{\text{square}} = 4(r^2 - x^2).$$

Hence

$$\frac{A_{\text{circle}}}{A_{\text{square}}} = \frac{\pi}{4}$$

and it follows that

$$\frac{V_{\text{sphere}}}{V_{\text{mouhefanggai}}} = \frac{\pi}{4}.$$

Hence the volume of the sphere is given by

$$\frac{\pi}{4} V_{\text{mouhefanggai}} = \frac{4}{3}\pi r^3.$$

4 Postscript

We could, of course, use calculus to obtain the volume of the móuhéfānggài:

$$V_{\text{mouhefanggai}} = \int_{-r}^{r} \int_{-\sqrt{r^2-z^2}}^{\sqrt{r^2-z^2}} \int_{-\sqrt{r^2-z^2}}^{\sqrt{r^2-z^2}} dx\,dy\,dz = \frac{16}{3} r^3$$

but this is far less elegant.

Even worse, we could use our favourite CAS package! The MATLAB code is as follows.

```
int(int(int(1,-sqrt(r^2-z^2),sqrt(r^2-z^2)),
        -sqrt(r^2-z^2),sqrt(r^2-z^2)),-r,r)
```

5 References

Boyer, C. B. (1968), *A History of Mathematics*, Wiley.

Brunton, J. (1973), The cube dissected into three yángmǎ, *Math. Gazette*, **57**, 66–67.

Heath, T. L. (2002), *The Works of Archimedes*, Dover.

Kiang, T. (1972), An old Chinese way of finding the volume of a sphere, *Math. Gazette*, **56**, 88–91.

Lam, L.-Y. and Shen, K. (1985), The Chinese concept of Cavalieri's principle and its applications, *Historia Mathematica*, **12**, 219–228.

McCaughan, E. (2001), Mouhefanggai, *Nrich*, **1412**, `https://nrich.maths.org/1412`, accessed 13/05/2021.

Polster, B. (2004), *Q.E.D. Beauty in Mathematical Proof*, Walker.

Pritchard, C. (ed.) (2003), *The Changing Shape of Geometry*, Cambridge University Press.

Wikipedia (2021a), `https://en.wikipedia.org/wiki/Archimedes_Palimpsest`, accessed 13/05/2021.

Wikipedia (2021b), `https://en.wikipedia.org/wiki/Cavalieri%27s_principle`, accessed 13/05/2021.

6 Appendix

In Figure 9 we show a template for the yángmǎ in a unit cube.

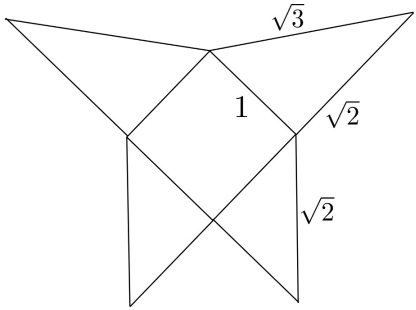


Figure 9: Yángmǎ, one third of a cube.

Problem 301.1 – Power sum

Tony Forbes

Let b and k be integers greater than 1. Show that

$$S(b,k) \;=\; \sum_{i=0}^{\infty} \frac{1}{\displaystyle\sum_{j=0}^{k-1} b^{ki+j}} \;=\; \frac{(b-1)\,b^k}{(b^k-1)^2}.$$

For example,

$$S(2,2) \;=\; \frac{1}{1+2} + \frac{1}{4+8} + \frac{1}{16+32} + \ldots \;=\; \frac{4}{9},$$

$$S(10,3) \;=\; \frac{1}{1+10+100} + \frac{1}{1000+10000+100000} + \ldots \;=\; \frac{1000}{110889}.$$

Solution 296.1 – Divisibility

Let m and n be positive integers with $m \geq 4$. Show that

$$(mn)! - m!\,(n!)^m \;\equiv\; 0 \pmod{n^{m+3}},$$

or find a counter-example.

Ted Gore

Let

$$p \;=\; \frac{(mn)!}{(n!)^m m!}.$$

Then

$$(mn)! - m!(n!)^m \;=\; m!(n!)^m(p-1).$$

I use an example to demonstrate that $(mn)!$ is divisible by $m!(n!)^m$. For $(m,n) = (4,5)$ we get

$$20! \;=\; (20\cdot 19\cdot 18\cdot 17\cdot 16)(15\cdot 14\cdot 13\cdot 12\cdot 11)(10\cdot 9\cdot 8\cdot 7\cdot 6)(5\cdot 4\cdot 3\cdot 2\cdot 1).$$

Taking the largest value from each set we get

$$20! \;=\; 4!\cdot 5^4(19\cdot 18\cdot 17\cdot 16)(14\cdot 13\cdot 12\cdot 11)(9\cdot 8\cdot 7\cdot 6)(4\cdot 3\cdot 2\cdot 1).$$

Each set of four consecutive numbers is divisible by $4!$. So $20! = 4!\cdot(5!)^4 p$, where $p = (19\cdot 3\cdot 17\cdot 4)(7\cdot 13\cdot 11)(9\cdot 2\cdot 7)$. Note that p is not divisible by 5. In this case $p - 1 = 782183\cdot 5^4$.

We need to show that $m!(n!)^m(p-1) \equiv 0 \pmod{n^{m+3}}$. Let

$$G(m,n) \;=\; \left\lfloor \frac{m}{n} \right\rfloor + \left\lfloor \frac{m}{n^2} \right\rfloor + \left\lfloor \frac{m}{n^3} \right\rfloor + \ldots,$$

where $\lfloor\ \rfloor$ is the floor of its argument.

If n is prime then G returns the highest power of n that divides $m!$. When n is compound then the highest power of n may be greater than G.

We can say immediately that $G(m,n) \geq 3$ if $m \geq 3n$ or if $m \geq n^2$. What about other combinations of m and n?

Let $m!(n!)^m = xn^{m+b+f}$, where $b = G(m,n)$ and f is the power of n in $m!(n!)^m$ generated by the factors of n less than n itself.

Let $p = yn^c + k$, so that $p - 1 = yn^c + k - 1$. Let

$$(mn)! - m!(n!)^m \;=\; zn^d \;=\; xn^{m+b+f}(p-1).$$

If $k = 1$, then $zn^d = xn^{m+b+f}yn^c$, so that $d = m + b + f + c$. Otherwise $zn^d = xn^{m+b+f}(p-1)$, so that $d = m + b + f$.

We need to show that $zn^d \equiv 0 \pmod{n^{m+3}}$.

It's easily seen that the condition is true for $n = 4$. For all compound $n > 4$, Wilson's theorem tells us that $(n-1)! \equiv 0 \pmod{n}$, so that $f \geq m$. Therefore we need to show that, for a prime, if $b + f < 3$ then $k = 1$ and $c \geq 3 - (b + f)$.

I use $(4, 5)$ to demonstrate that k always equals 1 for an odd prime n. To obtain q_t we start with the subset that has tn as its highest value and remove that value. So we take the first subset $(20 \cdot 19 \cdot 18 \cdot 17 \cdot 16)$ and remove the first value to give

$$q_4 = (19 \cdot 18 \cdot 17 \cdot 16) = (20-1)(20-2)(20-3)(20-4) = \alpha(5) + 4!,$$

where $\alpha(n)$ denotes a polynomial such that each term is divisible by at least n. We know that q_4 is divisible by 4! so that $\alpha(5)$ is divisible by 4!.

This procedure can be carried out for each subset to give

$$\begin{aligned} p &= \frac{(19 \cdot 18 \cdot 17 \cdot 16)(14 \cdot 13 \cdot 12 \cdot 11)(9 \cdot 8 \cdot 7 \cdot 6)(4 \cdot 3 \cdot 2 \cdot 1)}{(4!)^4} \\ &= (3875 + 1)(1000 + 1)(125 + 1) \\ &= (31 \cdot 5^3 + 1)(8 \cdot 5^3 + 1)(5^3 + 1). \end{aligned}$$

We see now that p actually equals $\alpha(5^3) + 1$ and we might expect c to be 3. In fact, $p - 1 = 782183 \cdot 5^4$ which satisfies the condition $c \geq 3$.

We need to show that, for an odd prime $n > 3$, $c \geq 3$. Taking

$$q_t = (tn-1)(tn-2)(tn-3)(tn-4),$$

where $n = 5$, we have

$$q_t = t^4n^4 - 10t^3n^3 + 35t^2n^2 - 50tn + 24.$$

Obviously every term but the constant term is divisible by n^3.

With $q_t = (tn-1)(tn-2)(tn-3)(tn-4)$ the expansion of the term in n is

$$-4!\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}\right)tn = -50tn = -2tn^3.$$

And the expansion of the term in n^2 is

$$4!\left(\frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \frac{1}{12}\right)t^2n^2 = 35t^2n^2 = 7t^2n^3.$$

These results suggest two conjectures. For primes greater than 3,

$$(n-1)!\sum_{i=1}^{n-1}\frac{1}{i} \text{ is divisible by } n^2, \text{ and}$$

$$(n-1)!\sum_{1\le i<j\le n-1}\frac{1}{ij} \text{ is divisible by } n.$$

I have confirmed they are true for the primes from 5 up to 1999. If the two conjectures are accepted, then for all primes $n > 3$, we have $c \geq 3$.

A similar procedure for $n = 3$ shows that $b \geq 1$ and $c \geq 2$. For $n = 2$, we have $b \geq 3$ and $c \geq 1$.

Now the coefficients 50 and 35 are Stirling numbers of the first kind; 50 being $s(5, 2)$ and 35 being $s(5, 3)$.

The conjectures become that $s(n, 2)$ is divisible by n^2 and $s(n, 3)$ is divisible by n. Wolstenholme's theorem is proof of the first. I have not found a specific proof of the second.

Tommy Moorhouse

Our strategy is to extract factors of n before proving that a certain sum is divisible by n, leading to the stated result. We first set out some lemmas.

Lemma 1 If n is composite then $(n-1)! \equiv 0 \pmod{n}$.

Proof If $n = ab$ for integers a and b both greater than 1, then a and b are both smaller than $n-1$ and so both are factors of $(n-1)!$. Hence n is also a factor. $\square$

Lemma 2 If n is a prime greater than 3 then $\sum_{k=1}^{n-1} k^2 \equiv 0 \pmod{n}$.

Proof This follows from the expression for the sum of consecutive squares

$$\sum_{k=1}^{n-1} k^2 = \frac{1}{6}n(2n-1)(n-1).$$

Since n is prime it is easily checked that the term $(2n-1)(n-1)$ is divisible by 6, so that the sum is divisible by n. $\square$

Now we expand the expression

$$(nm)! \;=\; nm(nm-1)\cdots n(m-1)\cdots n(m-k)\cdots n(n-1)\cdots 2\cdot 1.$$

We can extract a factor $n^m m!$ to leave $n^m m!\, Q(m,n)$ where

$$\begin{aligned}
Q(n,m) &= (nm-1)(nm-2)\cdots(n(m-1)+1)(n(m-1)-1)\cdots \\
&= \bigl(n^2(m-1)^2-(n-1)^2\bigr)\bigl(n^2(m-1)^2-(n-2)^2\bigr)\cdots \\
&\qquad\qquad\cdots\bigl(n^2(m-1)^2-1^2\bigr) \\
&\times \bigl(n^2(m-3)^2-(n-1)^2\bigr)\bigl(n^2(m-3)^2-(n-2)^2\bigr)\cdots \\
&\qquad\qquad\cdots\bigl(n^2(m-3)^2-1^2\bigr) \\
&\times \cdots \\
&\times \bigl(n^2-(n-1)^2\bigr)\bigl(n^2-(n-2)^2\bigr)\cdots\bigl(n^2-1^2\bigr).
\end{aligned}$$

Here we have matched up terms either side of the 'holes' in $Q(m,n)$ at $n(m-(2k+1))$, i.e. the terms

$$n(m-(2k+1)+j) \;\text{ and }\; n(m-(2k+1)-j),$$

where $j=1,2,3,\ldots,n-1$, to get the terms

$$n^2(m-(2k+1))^2-j^2.$$

A sketch might help to see what is happening: here the (singly or doubly) starred terms are matched, shown next to the 'holes'.

$$nm * \cdots n(m-1)\cdots * n(m-2) ** \cdots n(m-3)\cdots ** n(m-4)\cdots$$

If m is even then all the terms match up this way to give a product of differences of two squares. If m is odd we can match all the terms except those less than n, which leaves us with an extra factor of $(n-1)!$. In the expression for $Q(m,n)$ we see that if we multiply out the final terms in each of the brackets we get $(n-1)!^m$, taking into account the final $(n-1)!$ in the case of odd m. This cancels with the $(n-1)!^m$ in $Q(m,n)-(n-1)!^m$, so we can concentrate on the other terms in $Q(m,n)$.

We don't need to expand out the whole of $Q(m,n)$, but simply note that the terms that miss out exactly one of the final terms in the main brackets bring a factor of n^2. Reducing $Q(m,n)-(n-1)!^m$ modulo n^3 we have

$$n^2\sum_{k=1}^{[m/2]}(m-(2k-1))^2(n-1)!^m\sum_{j=1}^{n-1}\frac{1}{(n-j)^2}.$$

We can ignore the sum involving m here. We consider the term

$$(n-1)!^m\sum_{j=1}^{n-1}\frac{1}{j^2}\pmod{n},$$

which contains the same terms as that above, modulo n. The inverted terms can be resolved using the fact that, for prime n and any $j<n$ there is a unique $j'<n$ such that $jj'\equiv 1\pmod{n}$. Thus the final sum can be rewritten (mod n) as

$$\sum_{j=1}^{n-1}j^2\pmod{n}$$

which, by Lemma 2, is congruent to zero modulo n. Thus, since we have shown that

$$Q(m,n)-(n-1)!^m\ \equiv\ 0\ (\mathrm{mod}\ n^3)$$

if n is prime, we see that n^{m+3} divides $(nm)!-m!(n!)^m$. If n is composite we use Lemma 1 to reach the same conclusion more directly.

Problem 301.2 – Reciprocal sum

Ted Gore

Show that if n is prime and $n>3$, then

$$(n-1)!\sum_{i=1}^{n-1}\frac{1}{i}\ \equiv\ 0\ (\mathrm{mod}\ n^2)$$

and

$$(n-1)!\sum_{1\le i<j\le n-1}\frac{1}{ij}\ \equiv\ 0\ (\mathrm{mod}\ n).$$

See page 17 for the next problem of this type.

Solution 286.5 – Factorization

Given a positive integer n, denote by $\phi(n)$ the number of positive integers $m < n$ such that $\gcd(m,n) = 1$. If we know the complete factorization of n, say $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$ with positive integers $a_1, a_2, \ldots, a_r$ and distinct primes $p_1, p_2, \ldots, p_r$, we can easily compute

$$\phi(n) \;=\; (p_1 - 1)p_1^{a_1-1}\,(p_2 - 1)p_2^{a_2-1}\,\ldots\,(p_r - 1)p_r^{a_r-1}.$$

Is this process reversible? Given n and $\phi(n)$, is it possible to construct the complete factorization of n without too much difficulty? If it is, try factorizing

$n =$ 1586 02481 31293 11974 04552 75968 73607 71145 55549 11334 22976 68001 07012 76942 47700 99421 02756 52867 12646 06754 07200 60245 86133 22978 29252 68997 66323 73467 11294 88572 28050 70734 96620 00789 92252 73781

given that

$\phi(n) =$ 1586 02481 31293 11974 04552 75968 61357 52500 38117 66204 95814 65893 63834 77320 84117 64608 84450 72128 92453 11845 67688 17202 39729 99520 14675 73124 90380 04713 14884 75595 39954 75897 02033 54901 63971 74000.

Peter Fletcher

If we try Maple's `ifactor` on n or $\phi(n)$, Maple gets stuck, so we need a different method.

Let N be some integer and consider $N - \Phi(N)$. If q_1, q_2 and q_3 are the prime factors of N with multiplicities a, b and c, then

$$N - \Phi(N) \;=\; q_1^a\, q_2^b\, q_3^c - (q_1 - 1)q_1^{a-1}(q_2 - 1)q_2^{b-1}(q_3 - 1)q_3^{c-1}.$$

If now we expand this and divide by N, we get

$$\frac{N - \Phi(N)}{N} \;=\; \frac{q_1 q_1 + q_1 q_3 + q_2 q_3 - q_1 - q_2 - q_3 + 1}{q_1\, q_2\, q_3}.$$

Note that the denominator is the product of the prime factors ignoring the multiplicities. If now $b = 1$ and $c = 1$ and we divide N by $q_1\, q_2\, q_3$, the result will be q_1^{a-1}.

Turning to the question, it turns out that if we let the denominator of $\bigl(n - \phi(n)\bigr)/n$ be d and find n/d, this is an integer that happens to be a square of a prime: let this prime be p_1. Since p_1 appears in d exactly once, we know that p_1^3 divides n.

Let

$$n_1 \;=\; \frac{n}{p_1^3} \qquad \text{and} \qquad \phi_1(n_1) \;=\; \frac{\phi(n)}{(p_1 - 1)p_1^2}.$$

We know that the rest of the prime factors of n, let them be $p_2, p_3, \ldots$, each appear in n_1 exactly once. This means that we must have

$$\phi_1(n_1) \; = \; (p_2 - 1)(p_3 - 1) \cdots .$$

We can still not use Maple's `ifactor` on n_1, but we can use it on $\phi_1(n_1)$: the result is 20 prime factors, 2 appearing three times. Each $(p_i - 1)$ is even, so there could be up to three more primes to find.

Let the prime factors of $\phi_1(n_1)$ be denoted $f_1, f_2, \ldots f_{20}$. A certain product of some of these, including at least one 2, will equal $(p_2 - 1)$, so if we then add 1 we shall get p_2.

We can loop through each of

$$f_i + 1, \quad f_i f_j + 1, \quad f_i f_j f_k + 1, \quad \ldots$$

in turn, for $i, j, k, \ldots = 1, 2, \ldots, 20$ and test each product+1 to see if it is prime. If it is, we can then see if it divides n_1. If we do this, we very soon find $(p_2 - 1)$ with five prime factors and hence p_2.

Let $n_2 = n_1/p_2$. Maple's `ifactor` does now work on n_2 and the result is p_3 and p_4.

To summarise, $n = p_1^3\, p_2\, p_3\, p_4$, where n is per the question and

$$\begin{aligned} p_1 &= 466435879660522367654413675211, \\ p_2 &= 562422394447827908154562532159, \\ p_3 &= 494179332730633784520908832239, \\ p_4 &= 562324418721793120042174985351. \end{aligned}$$

Problem 301.3 – Integers

Tony Forbes

For some integer $q \geq 1$, there are $q + 1$ non-negative integers, n_1, n_2, …, n_{q+1} that satisfy

$$q + \sum_{i=1}^{q+1} n_i \; = \; \sum_{i=1}^{q+1} i\, n_i \; = \; \sum_{i=1}^{q+1} i(i-1) n_i \; = \; q^2 + q.$$

Show that $n_1 = q^2 - 1$ and $n_{q+1} = 1$.

Lines in $\mathbb{R}^3$ and vector fields on S^2

Tommy Moorhouse

This investigation concerns a correspondence between sets of lines in $\mathbb{R}^3$ and vector fields on the 2-sphere S^2. If we fix an origin in $\mathbb{R}^3$, real three-dimensional space, we can characterise all its directed lines using pairs of vectors as follows. Let $\vec{v}$ be the unique vector based at the origin meeting the line at right angles. Then let $\vec{u}$ be a unit vector pointing along the line from the tip of $\vec{v}$, defining the direction of the line. The pair $(\vec{v}, \vec{u})$ completely specifies the directed line. We have the conditions $\vec{v} \cdot \vec{u} = 0$, and $\vec{u} \cdot \vec{u} = 1$.

This specification can be used to define vector fields on part or (more interestingly) all of S^2. Given $(\vec{v}, \vec{u})$ the unit direction vector $\vec{u}$ gives a point of S^2 and we define the tangent vector at this point to be $\vec{v}$. By construction $\vec{v}$ is tangent to the sphere at the point defined by $\vec{u}$.

It is interesting to see what the correspondence looks like. Try sketching a set of lines (part of a ruled surface for example) and mark the corresponding vector field on a sketch of part of a sphere, or take your favourite vector field on S^2 and see what the corresponding set of lines in $\mathbb{R}^3$ looks like. Keep in mind that $\vec{v}$ and $\vec{u}$ must be perpendicular. One set of corresponding configurations is shown in Figure 1, where the lines (each line representing a pair of oppositely directed lines) pass through a single point P distinct from the origin, and the vector field vanishes at the poles but generally points 'north'.

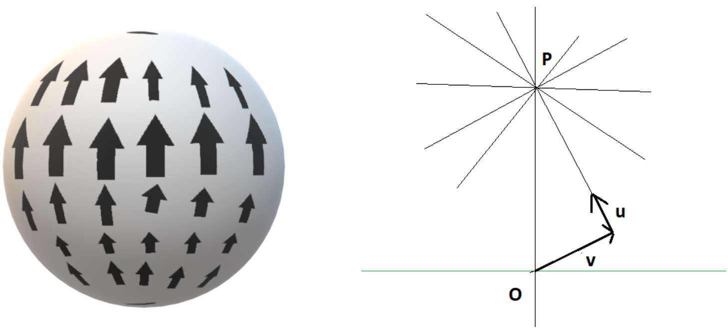


Figure 1: Vector field on sphere and some of the corresponding lines.

Rotations of $\mathbb{R}^3$ fixing the origin also change the vector field on S^2 –

perhaps you can investigate how. What happens if the origin is changed but the set of lines remains fixed? For example, in the case depicted in Figure 1 what happens when P is moved downwards to eventually coincide with the origin? With the origin fixed any point P determines a vector field on S^2 through the set of lines passing through it.

Let us call a set of lines that gives rise to a smooth vector field with isolated zeros on S^2 through the above correspondence 'allowed'. What properties must an allowed set of lines have to ensure that the corresponding set of vectors forms a smooth vector field on the whole of S^2? Deduce from the properties of smooth vector fields on S^2 that any allowed set contains at least one directed line through the origin. Is the origin special or does any allowed set include at least one directed line passing through any given point of $\mathbb{R}^3$?

Note The construction in this article was used by N. J. Hitchin to construct solutions to a set of equations arising in physics, and by others in the study of surfaces.

Problem 301.4 – Triple reciprocal sum

Tony Forbes

(i) Suppose n is odd. Either show that

$$(n-1)! \sum_{1 \le i < j < k \le n-1} \frac{1}{ijk} \;\equiv\; 0 \pmod{n},$$

or find a counter-example.

(ii) Let n be a positive integer and let

$$H_s(n) \;=\; 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s}.$$

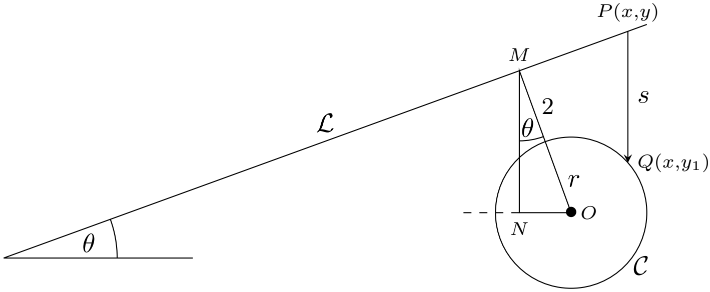
Show that for any positive integer n,

$$\sum_{1 \le i < j < k \le n} \frac{1}{ijk} \;=\; \frac{H_1(n)^3 - 3H_1(n)H_2(n) + 2H_3(n)}{6}.$$

This formula might be useful for dealing with (i). For not too large n, the Mathematica function `HarmonicNumber[n,s]` can be used to compute $H_s(n)$ very rapidly.

Solution 295.4 – A line and a circle

Richard Gould



Problem The line $\mathcal{L}$ makes an angle θ with the horizontal, where $0 < \theta < \pi/2$. A circle $\mathcal{C}$ lies below $\mathcal{L}$, separated from it by 2 m. A particle is dropped from a variable point P above $\mathcal{C}$ and falls under gravity a distance s to meet the circle at Q. Determine the fastest time of descent for the particle and show that it is independent of the radius of $\mathcal{C}$. Gravity is constant and acts vertically down.

Construction OM is the perpendicular from the centre of the circle, O, to $\mathcal{L}$. Drop a perpendicular from M to meet the horizontal line through O at the point N. The angle $O\widehat{M}N$ is equal to θ.

Solution Let the magnitude of the acceleration due to gravity be g. Using the standard notation and equations of motion for constant linear acceleration we have

$$v = gt, \quad v^2 = g^2t^2 = 2gs,$$

giving

$$t = \sqrt{\frac{2s}{g}}.$$

From which we see that, unsurprisingly, the fastest descent occurs when the vertical distance between the line and the circle is a minimum.

Establish a Cartesian coordinate system with origin at the centre of the circle O and let the radius of the circle be r m. The geometry of triangle OMN tells us that the coordinates of M are $(-(2+r)\sin\theta, (2+r)\cos\theta)$. Since $\mathcal{L}$ has gradient $\tan\theta$, the equation of $\mathcal{L}$ is

$$y - (2+r)\cos\theta = (x + (2+r)\sin\theta)\tan\theta,$$

from which

$$y = x\tan\theta + \frac{2+r}{\cos\theta},$$

The equation of the circle is, of course $x^2 + y^2 = r^2$. Referring to the diagram, we can now find the s-value for an arbitrary point $P(x, y)$ on $\mathcal{L}$.

$$s = y - y_1 = x \tan\theta + \frac{2 + r}{\cos\theta} - \sqrt{r^2 - x^2}.$$

To find the minimum distance we solve the equations

$$\frac{\partial s}{\partial x} = \tan\theta + \frac{x}{\sqrt{r^2 - x^2}} = 0, \qquad (1)$$

$$\frac{\partial s}{\partial r} = \frac{1}{\cos\theta} - \frac{r}{\sqrt{r^2 - x^2}} = 0, \qquad (2)$$

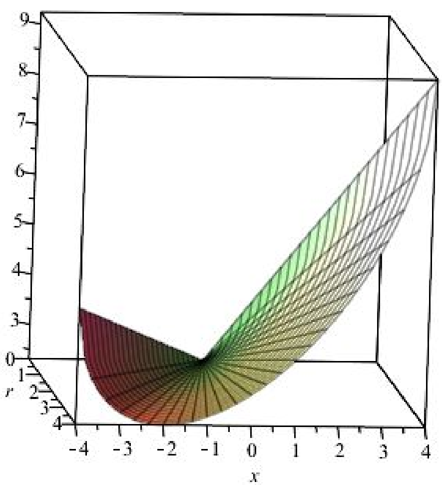
simultaneously. Equation (2) gives $x = \pm r \sin\theta$. Substituting into equation (1) gives

$$\tan\theta \pm \frac{r \sin\theta}{\sqrt{r^2(1 - \sin^2\theta)}} = 0 \quad \text{for } x = -r\sin\theta \text{ only.}$$

So there is a stationary point at $x = -r\sin\theta$. As this does not provide a constant solution for (r, x) there is no isolated local extremum. Indeed, the usual tests for classifying stationary points fail since the determinant of the Hessian matrix is zero (not demonstrated here) and the matrix itself has a zero eigenvalue.

A 3-D plot, generated by MAPLE, shows us what is going on.

Plot of $s(r, x)$ for $\theta = \pi/6$



From the plot we see that there is a minimum in the x-r plane (i.e. s constant) for each value of r and these all appear to lie in the same s-r plane. We can confirm the minimum by the second derivative test.

$$\frac{\partial^2 s}{\partial x^2} = \frac{\sqrt{r^2 - x^2} + \dfrac{2x^2}{2\sqrt{r^2 - x^2}}}{r^2 - x^2} = \frac{r^2}{(r^2 - x^2)^{3/2}} > 0,$$

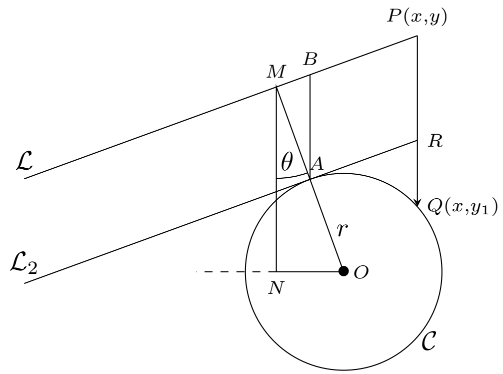
The minimum value of s and the resulting time of descent are given by

$$\begin{aligned} s_{\min} &= -r\frac{\sin^2\theta}{\cos\theta} + \frac{2+r}{\cos\theta} - r\cos\theta \\ &= \frac{2 + r - r(\sin^2\theta + \cos^2\theta)}{\cos\theta} = \frac{2}{\cos\theta}. \end{aligned}$$

And
$$t_{\min} = \frac{2}{\sqrt{g\cos\theta}},$$

which establishes that $t_{\min}$ is independent of r.

Footnote I learned a salutory lesson from this experience. I always advise my students to spend a few moments thinking about a problem before embarking on the obvious method of solution and reconsider their approach if the working becomes difficult. Although the above was far from intractable, I had a nagging feeling as I worked through it that there might be a simpler, geometric solution. I was in Covid-19 lockdown at the time and sharing puzzles with a friend and colleague who produced the following solution, having first demonstrated as above that the problem only required identification of the shortest descent path.



Construction Let OM instersect the circle at A. Draw $\mathcal{L}_2$, the tangent to the circle at A, intersecting PQ at R. Draw a vertical line through A to meet $\mathcal{L}$ at B.

Solution Since $\mathcal{L}_2$ is perpendicular to OM it is parallel to $\mathcal{L}$. From the point P the descent path to the circle is $PR + RQ$ but $PRAB$ is a parallelogram and so $PR = BA$. Since, for all points P on $\mathcal{L}$ above the circle, the distance RQ is positive or zero, the minimum descent is from B with a descent height of $BA = 2/\cos\theta$. The rest follows. Clearly this was an occasion when I should have followed my own advice!

Solution 280.3 – Digits

> List all the d-digit numbers in base $d+1$ (actually any base larger than d will do) that satisfy all of the following. (i) The digits are in non-increasing order reading left to right; (ii) the difference between consecutive digits is either 0 or 1; (iii) the units digit is 0 or 1. How long is the list?

Steve Moon

Let's start by working through a specific example. I chose base 5. Including zero as 0000, there are 16 four-digit numbers whose digits satisfy the three criteria.

0000 1110 1111 2221 1000 2110 2111 3221
1100 2210 2211 3321 2100 3210 3211 4321

There are 8 three-digit numbers in base 5 whose digits meet the criteria and these also provide the list of permitted three-digit numbers in base 4.

000 111 100 211 110 221 210 321

There are 4 two-digit numbers in base 5 meeting the requirements and these also provide the list of permitted two-digit numbers in bases 4 and 3.

00 11 10 21

We conjecture that the number of allowable d-digit numbers in base $d+1$ is 2^d. Furthermore, for any base $d+k$, $k>1$, the number of allowable d-digit numbers is 2^d. The reasoning is as follows: for base $d+1$, starting in the units column as required with either 0 or 1, each of these permits two options for entry into the next column. Then each entry in this second column permits two entries in the third column, and so on for up to d columns.

Problem 301.5 – Matrix powers

Tony Forbes

For integer $n \ge 3$, let A be an $n \times n$ matrix whose r-th row is $[0\ 1\ 0\ 0\ \ldots\ 0\ 1]$ rotated right by $r-1$ places. Show that for $h = 1, 2, \ldots, n-1$ and $i = 1, 2, \ldots, n$, we have

$$[A^h]_{i,i} \;=\; \begin{cases} 0 & \text{if } h \text{ is odd,} \\ \dbinom{h}{h/2} & \text{if } h \text{ is even.} \end{cases}$$

Can you extend this formula to $n \le h \le 2n-1$?

Solution 297.1 – Matrix square root

Suppose $n \in \{2, 3, 4, \dots\}$ and α, β are real numbers such that $\alpha - \beta \geq 0$ and $\alpha + (n-1)\beta \geq 0$. Let M be the $n \times n$ matrix whose diagonal entries are all α and whose other entries are all β. Find a square root for M, i.e. a matrix S such that $S^2 = M$.

Tommy Moorhouse

We can write the matrix M as $(\alpha - \beta)\mathbb{I} + \beta\mathbb{U}$ where $\mathbb{U}$ is the $n \times n$ of 1s. We observe that $\mathbb{U}^2 = n\mathbb{U}$. We look for a solution of the form $(\sqrt{\alpha - \beta})(\mathbb{I} + x\mathbb{U})$; that is,

$$\mathbb{I} + \frac{\beta}{\alpha - \beta}\mathbb{U} \;=\; (\mathbb{I} + x\mathbb{U})^2.$$

Expanding the right hand side we see that we must have

$$nx^2 + 2x - A \;=\; 0$$

where $A = \beta/(\alpha - \beta)$. Solving for x we have

$$x \;=\; \frac{1}{n}\left(\sqrt{nA + 1} - 1\right) \;=\; \frac{1}{n\sqrt{\alpha - \beta}}\left(\sqrt{\alpha + (n-1)\beta} - \sqrt{\alpha - \beta}\right).$$

Finally, the required square root is

$$\left(\sqrt{\alpha - \beta}\right)\mathbb{I} + \frac{1}{n}\left(\sqrt{\alpha + (n-1)\beta} - \sqrt{\alpha - \beta}\right)\mathbb{U}.$$

The conditions on α and β make both square roots real.

Reinhardt Messerschmidt

Let J and $\mathbf{1}$ be the all-1 matrix and all-1 column vector respectively, with their dimensions determined by the context. Note that $M = (\alpha - \beta)I + \beta J$. The diagonalization of M is

$$\begin{aligned} M \;&=\; \begin{bmatrix} 1 & \mathbf{1}^T \\ \mathbf{1} & -I \end{bmatrix} \begin{bmatrix} \alpha + (n-1)\beta & \mathbf{0}^T \\ \mathbf{0} & (\alpha - \beta)I \end{bmatrix} \begin{bmatrix} 1 & \mathbf{1}^T \\ \mathbf{1} & -I \end{bmatrix}^{-1} \\ &=\; \begin{bmatrix} 1 & \mathbf{1}^T \\ \mathbf{1} & -I \end{bmatrix} \begin{bmatrix} \alpha + (n-1)\beta & \mathbf{0}^T \\ \mathbf{0} & (\alpha - \beta)I \end{bmatrix} \begin{bmatrix} n^{-1} & n^{-1}\mathbf{1}^T \\ n^{-1}\mathbf{1} & n^{-1}J - I \end{bmatrix}. \end{aligned}$$

A square root for M is therefore

$$\begin{aligned} S \;&=\; \begin{bmatrix} 1 & \mathbf{1}^T \\ \mathbf{1} & -I \end{bmatrix} \begin{bmatrix} \sqrt{\alpha + (n-1)\beta} & \mathbf{0}^T \\ \mathbf{0} & (\sqrt{\alpha - \beta})I \end{bmatrix} \begin{bmatrix} n^{-1} & n^{-1}\mathbf{1}^T \\ n^{-1}\mathbf{1} & n^{-1}J - I \end{bmatrix} \\ &=\; (\sqrt{\alpha - \beta})I + n^{-1}(\sqrt{\alpha + (n-1)\beta} - \sqrt{\alpha - \beta})J. \end{aligned}$$

Stuart Walmsley

Introduction

The determinant corresponding to the matrix in this problem has been the subject of two previous problems, 282.5 and 283.2, to each of which I gave a solution, in issues **284** and **288** respectively. The same method can be used to solve the present problem. In square matrix M, the diagonal elements are all equal to α and the off diagonal elements to β. A matrix T, given in the earlier work, leads to D, a diagonal form of M:

$$TMT^{-1} \;=\; D \tag{1}$$

in which all $d_{j,k} = 0$ for $j \neq k$. The square root of D is then the diagonal matrix R in which each diagonal element is the square root of the corresponding element in D. Inverting (1),

$$T^{-1}DT \;=\; M, \quad T^{-1}RRT \;=\; M, \quad T^{-1}RTT^{-1}RT \;=\; M,$$

so that $T^{-1}RT = S$ is a square root of M.

The Transformation Matrix

It has been shown in the solutions to several previous problems that a matrix of the form M can be diagonalized by a matrix T, each element of which is proportional to an nth root of one, n being the dimension of the matrix. The matrix elements of T are most simply expressed if the rows and columns are labelled 0 to $n-1$. In what follows

$$e_j \;=\; \exp(2\pi ij/n), \quad j = 0, 1, \ldots, n-1.$$

and, in particular

$$e_{jk} \;=\; \exp(2\pi ijk/n).$$

From the general properties of roots of one, it is noticed that

$$e_0 \;=\; 1 \quad \text{and} \quad e_1 + e_2 + \cdots + e_{n-1} \;=\; -1.$$

Then

$$T_{j,k} \;=\; n^{-1/2} e_{jk}.$$

An element in the inverse matrix T^{-1} is given by

$$T^{-1}_{j,k} \;=\; T^*_{k,j}$$

in which $*$ represents the complex conjugate.

Solution

We have

$$
\begin{gathered}
M_{j,j} \;=\; \alpha, \qquad M_{j,k} \;=\; \beta, \quad j \neq k, \\
T_{j,k} \;=\; n^{-1/2}\exp(2\pi i jk/n), \\
D_{0,0} \;=\; \alpha + (n-1)\beta, \qquad D_{j,j} \;=\; \alpha - \beta, \quad j > 0, \\
R_{0,0} \;=\; \sqrt{D_{0,0}}, \qquad R_{j,j} \;=\; \sqrt{D_{j,j}}, \quad j > 0, \\
nS_{j,j} \;=\; R_{0,0} + (n-1)R_{1,1}, \qquad nS_{j,k} \;=\; R_{0,0} - R_{1,1}, \quad j \neq k, \\
M \;=\; S^2, \qquad \alpha \;=\; S_{j,j}^2 + (n-1)S_{j,k}^2, \qquad \beta \;=\; 2S_{j,j}S_{j,k} + (n-2)S_{j,k}^2.
\end{gathered}
$$

An Example

$$
\begin{gathered}
M_{j,j} \;=5, \qquad M_{j,k} \;=\; 1, \qquad n = 5, \\
D_{0,0} \;=\; 9, \qquad D_{1,1} \;=\; 4, \\
R_{0,0} \;=\; 3, \qquad R_{1,1} \;=\; 2, \\
S_{j,j} \;=\; 11/5, \qquad S_{j,k} \;=\; 1/5, \\
M_{j,j} \;=\; 121/25 + 4/25 \;=\; 5, \qquad M_{j,k} \;=\; 22/25 + 3/25 \;=\; 1.
\end{gathered}
$$

Another Example

$$
\begin{gathered}
M_{j,j} \;=\; 5, \qquad M_{j,k} \;=\; 2, \qquad n = 4, \\
D_{0,0} \;=\; 11, \qquad D_{1,1} \;=\; 3, \\
R_{0,0} \;=\; \sqrt{11}, \qquad R_{1,1} \;=\; \sqrt{3}, \\
S_{j,j} \;=\; \bigl(\sqrt{11} + 3\sqrt{3}\bigr)/4, \qquad S_{j,k} \;=\; \bigl(\sqrt{11} - \sqrt{3}\bigr)/4, \\
M_{j,j} \;=\; (38 + 42)/16 \;=\; 5, \qquad M_{j,k} \;=\; (4 + 28)/16 \;=\; 2.
\end{gathered}
$$

Problem 301.6 – Almost skew-symmetric matrix

Tony Forbes

Let M be a square matrix of dimension n with integer entries such that $M_{i,j} = -M_{j,i}$ for $1 \le i, j \le n$ except for one of the diagonal entries, $i = j = d$ say, in which case $M_{d,d} = p$.

Show that (i) when n is even the determinant of M is a square; (ii) when n is odd the determinant of M is pq^2 for some integer q.

Problem 301.7 – Legendre symbol sum

Tony Forbes

Suppose p is prime and $p \equiv 5 \pmod{24}$. Show that

$$\sum_{n=1}^{(p-1)/6} n \left(\frac{n}{p}\right) \;=\; 0,$$

where $\left(\frac{n}{p}\right)$ is the Legendre symbol. In case it might be useful, recall that when $1 \le n < p$ we have $\pm 1 = \left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod{p}$. More generally, find (a, m, d) such that

$$\sum_{n=1}^{(p-1)/d} n \left(\frac{n}{p}\right) \;=\; 0 \quad \text{for prime } p \equiv a \pmod{m}. \tag{1}$$

For example, (1) holds when $(a, m, d) = (1, 4, 1)$ since

$$\left(\frac{-1}{p}\right) \;=\; 1 \quad \text{and hence} \quad n\left(\frac{n}{p}\right) + (-n)\left(\frac{-n}{p}\right) \;=\; 0.$$

The triple $(a, m, d) = (7, 8, 2)$ occurs in $\mathbb{QARCH}$ **112** (2019). Apart from silly cases, such as $(0, 2, 2)$ for example, and trivial extensions of $(1, 4, 1)$, $(7, 8, 2)$ and $(5, 24, 6)$, such as $(847, 960, 2)$ for example, I do not know of any others.

Problem 301.8 – Prime product

Tony Forbes

Let P_n denote the n-th prime. Consider the product

$$F(N) \;=\; \prod_{i=0}^{N} \frac{P_{4i+1}}{P_{4i+2}} \frac{P_{4i+4}}{P_{4i+3}}.$$

Thus

$$F(0) = \frac{2}{3} \cdot \frac{7}{5} = 0.933333,\; F(1) = \frac{2}{3} \cdot \frac{7}{5} \cdot \frac{11}{13} \cdot \frac{19}{17} = 0.882655,\; F(2) = 0.835527,$$

and so on. Can $F(N)$ ever exceed 1?

04.00

Problem 301.9 – Integral

Show that

$$\int_0^1 \frac{\sqrt{1-x^2}}{\sqrt{1+x^2}}\,dx \;=\; \frac{\Gamma(1/4)^4 - 8\pi^2}{4\sqrt{2\pi}\,\Gamma(1/4)^2}.$$

Front cover Pentagonal geometry PENT(2,14,10) [`https://arxiv.org/abs/2104.02760`].