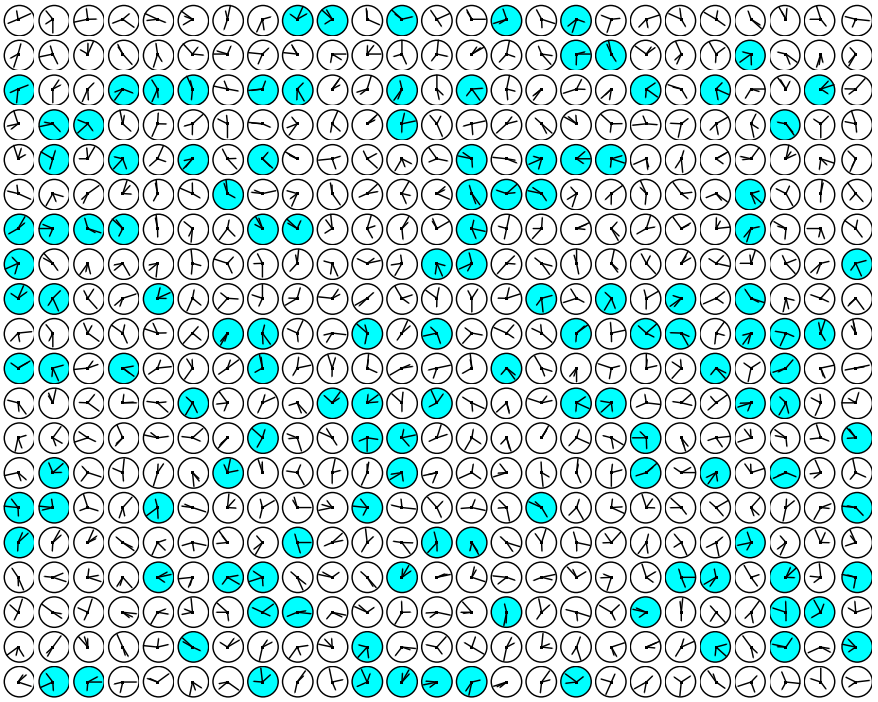
*

ISSN 1350-8539

M500 257



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 May Weekend is a residential Friday to Sunday event providing revision and examination preparation for both undergraduate and postgraduate students. For full details and a booking form see m500.org.uk/may.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. For details see m500.org.uk/winter.htm.

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 the Editor, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation.

Lottery tickets

Tony Forbes

Perhaps some of you followed that excellent television program [1] involving Dara O Briain, Marcus du Sautoy and two teams of invited celebrities engaging in mathematical problem-solving competitions. The idea is that one team always uses trial and error, intuition, magic and other similar methods to feel their way towards the answer to the given question whereas their opponents must resort to mathematics and logic. Curiously, as the game progresses it is not usually obvious which side has the better chance of winning. On one occasion they were required to

> find the minimum number of tickets you need to buy to guarantee a win in a lottery where (i) there are 14 numbered balls, (ii) you choose three numbers, (iii) three balls are drawn by the lottery machine and (iv) you win if and only if you match two or more numbers.

Both teams failed to answer the question and it was left for Marcus du Sautoy to reveal a 14-ticket solution involving two $S(2,3,7)$s. Construct a Steiner system $S(2,3,7)$ on the points $\{1,2,\ldots,7\}$, say

$$\{\{1,2,4\},\ \{2,3,5\},\ \{3,4,6\},\ \{4,5,7\},\ \{5,6,1\},\ \{6,7,2\},\ \{7,1,3\}\},\quad (*)$$

and purchase 7 tickets corresponding to its 7 triples. By definition [2] this will cover each of the 7 choose 2 pairs from $\{1,2,\ldots,7\}$. Do the same for $\{8,9,\ldots,14\}$ by adding 7 to the numbers in $(*)$. So now you have 14 tickets. The three balls are drawn. They must contain at least two small numbers or at least two large numbers. And since you are covered for each of these possibilities, you are guaranteed a prize. But if I remember correctly, only one half of the problem was solved. So I offer the other half to M500 readers: Do 13 tickets suffice to guarantee a prize in the 14-ball lottery?

Whilst watching the programme it occurred to me (and to many others I expect) that there exists a Steiner system $S(3,6,22)$. And moreover it might have some relevance to the UK lottery with its 49 balls, where you choose six numbers, they draw six balls and a ticket wins if and only if it matches at least three numbers.

Now imagine temporarily that the number of balls is reduced to 44, an even number that is two times 22. As a simple calculation shows, a Steiner system $S(3,6,22)$ consists of (22 choose 3)/(6 choose 3) = 77 sextuples and contains each of the 22 choose 3 = 1540 triples. So you can buy 77 tickets to cover numbers in the set $A = \{1,2,\ldots,22\}$ and a prize is guaranteed if

the draw contains three numbers from this set. Similarly another 77 tickets will cover the set $B = \{23, 24, \ldots, 44\}$. But amongst the six balls drawn there must be three A numbers or three B numbers (or both). Therefore at least one of your 154 tickets will win a prize.

We will need to exhibit an actual Steiner system $S(3, 6, 22)$ to make this work. Writing out 77 sextuples will take a lot of space. Fortunately there exist systems generated from a set of starter blocks under the action of the mapping $z \mapsto z + 2 \pmod{22}$. To see how this might work, you can confirm that $7 \cdot 22/2 = 77$. Take these seven blocks,

$$\{0,1,2,3,6,19\},\ \{0,1,5,8,12,13\},\ \{0,1,7,9,14,16\},\ \{0,2,4,7,12,18\},$$
$$\{0,2,11,13,14,21\},\ \{0,3,4,9,10,13\},\ \{0,3,5,7,11,17\},$$

and apply $z \mapsto z + 2 \pmod{22}$ to create seven distinct orbits of 11 blocks each. When you use this system to buy your lottery tickets you must of course remember to add 1 and 23 to cover the numbers 1–22 and 23–44 respectively.

Well, that's very nice, but the UK lottery still has 49 balls. Fortunately there also exists a Steiner system $S(3, 6, 26)$ [3], and in a similar manner we can use its 130 blocks to make (26 choose 3)/(6 choose 3) = 130 tickets from the set $B' = \{23, 24, \ldots, 48\}$ bringing the total to 77 + 130 = 207. This works extremely well. We don't have to worry about the missing number, for if the draw includes 49, the other five balls will still contain either three A numbers or three B' numbers.

However, 207 is rather large; so instead we shall try to extend the two $S(3, 6, 22)$ method. Divide the numbers into three sets

$$A = \{1, 2, \ldots, 22\},\quad B = \{23, 24, \ldots, 44\},\quad C = \{45, 46, \ldots, 49\},$$

use the $S(3, 6, 22)$ for A and B and purchase one more ticket,

$$\{1, 45, 46, 47, 48, 49\}.$$

Now we are covered if the draw contains three As or three Bs or three Cs and so the only pattern that might cause trouble is $\{A, A, B, B, C, C\}$.

One simple way of patching things up is to buy another 20 tickets,

$$\{n, 45, 46, 47, 48, 49\},\quad n = 2, 3, \ldots, 21,$$

which brings the total to 175. Since the draw contains two A numbers we do not need $n = 22$.

I am certain that 175 is not optimal. There ought to be a better alternative to the wasteful 21-fold repetition of the five C numbers. But I shall gladly leave it for others to construct a superior strategy. So here is another problem for you to solve.

> Find a set of less than 175 UK National Lottery tickets that guarantees a prize.

A far as I am aware the minimum number is not known.

Finally, I suppose I ought to explain that using the two $S(3,6,22)$s method for purchasing lottery tickets is not a sensible thing to do in real life—unless you are feeling very charitable. The UK lottery's terrible odds still apply and you will not necessarily recover your costs.

Notes

[1] *School of Hard Sums*, first broadcast on Dave in 2012.

[2] Recall from M500 **195**, or elsewhere, that a *Steiner system* $S(t,k,v)$ consists of a pair $(V,\mathcal{B})$, where V is a v-element set and $\mathcal{B}$ is a collection of k-element subsets of V, usually called *blocks*, or *lines* if the system has some geometric significance, with the property that each t-element subset of V is contained in precisely one block. For the $S(2,3,7)$ at the beginning, V is the set $\{1,2,3,4,5,6,7\}$ and

$$\mathcal{B} \;=\; \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}\}.$$

In this example each line has three points and a point occurs at the intersection of three lines, The system corresponds to a finite projective plane of order 2. Observe also that the system is cyclic—it can be generated from $\{1,2,4\}$ under the action of $z \mapsto z+1 \pmod 7$ on identifying 0 and 7. The interested reader is invited to draw the thing on a sheet of paper, representing the points as dots and the blocks as (not necessarily straight) lines. And you might like to prove by constructing it from scratch (or otherwise) that the $S(2,3,7)$ is unique up to isomorphism.

[3] A Steiner system $S(3,6,26)$ can be built from these ten blocks,

{0,1,2,4,7,13}, {0,1,3,12,19,21}, {0,1,5,9,10,16}, {0,1,6,8,15,24},
{0,1,11,17,18,22}, {0,1,14,20,23,25}, {0,2,6,14,19,22},
{0,2,12,15,16,23}, {0,3,13,15,18,25}, {0,5,13,17,19,23},

by applying $z \mapsto z+2 \pmod{26}$ to make ten 13-block orbits.

Trouble with infinity

Ken Greatrix

After reading an article by Sebastian Hayes, Contra Cantor, M500 **223**, pp 1–9, I realize that I'm not the only one to question the theory of something existing beyond infinity. Here's my version of the situation, in which I also describe the confusion I experienced with the mathematical concept of infinity.

When I was a small boy at primary school, we didn't have infinity. We had sums, and multiplication tables, and fractions, and percentages, and take-aways (not the burger and chips variety), and decimals. Life was much simpler then, and all seemed to be getting along fine.

At secondary school we became more formal, with arithmetic, algebra and geometry. So just when I was beginning to feel we were now getting into proper maths, problems started to rear their ugly heads to spoil the fun.

In the geometry class, the teacher told us about parallel lines, the statement being in the true Euclidean fashion that parallel lines never meet, no matter how far they are produced. This was OK so far, but then an older boy from a higher year told me quite authoritatively that parallel lines meet at infinity. Aside from this being a contradiction of the geometry teacher's information, and not knowing much about these things at that time, I conjured up a vision of a machine with a continuous strip of paper passing over a rotating drum, with two pencils clamped a set distance apart. When infinity was eventually achieved (I had a very vivid imagination then!), the two pencils would magically collide. Disregarding the magic, how can these clamped pencils loosen themselves and then collide; thus causing the parallel lines to 'meet at infinity'? By taking the simplistic (or Euclidean) view, two lines either converge at a point with an angle which is always apparent, diverge from a point with an equally apparent angle or they don't meet at all.

Leaving the geometry aside, at some stage during the advanced arithmetic classes we were given the impression that infinity was a very big number and then some more. Not a very good definition here, but even more confusingly; *'one divided by zero equals infinity'* and *'one divided by infinity equals zero'*.

After leaving school I went to college as part of an engineering apprenticeship scheme. The above definition of infinity was debunked by the maths lecturer. Extending the above statement, he went on to say that *'Also note*

that two divided by infinity equals zero, therefore two equals one. This is a contradiction. Hence infinity is not a number and should not be treated as such.' (Which incidentally is why I didn't express the above statements in strict mathematical symbolic language.) Unfortunately, this spark of clarity was just as quickly extinguished. This was because also during this same session, he went on to talk about the Aleph-Null, and the myriad of infinities which follow on from it.

So far, this is not a very good start for a budding mathematician (which I thought of becoming later on; at this particular time I was trying to become an electrical engineer). I wonder if other students have been similarly confused by these awkward definitions in their early maths life.

I am pleased to report that things begin to pick up some time later. Several years after finishing my apprenticeship training and its associated further education, I enrolled with the OU.

The concept of infinity that is appropriate here as a property of positive integers is:

If a number n exists, then so does the number $n + 1$.

The Archimedean principle.

Thus, if we are able to describe any number, n, by counting from 0 we then have a set of values, a_0, such that $0 \leq a_0 < n$. So we begin to see the concept of the counting numbers being boundless.

This principle is extended into the account of Hotel Hilbert (David Hilbert, 1862–1943). This hotel has an infinite number of rooms with an infinite number of guests in residence. When another guest arrives, all the existing guests are moved up one room—leaving the first room empty for the newcomer.

Although I find the concept of Hotel Hilbert acceptable, the associated explanation that *'infinity-plus-one is still infinity'* doesn't seem to follow on from the Archimedean Principle. But this is yet another example of the misuse of infinity. If $n + 1 = n$, should we assume that $n = \infty$? By simple algebraic manipulation we get $1 = 0$, which is just another contradiction.

Returning to the above counting scheme:

If $n + 1$ exists, then so does $(n + 1) + 1$; (or $n + 2$).

If $n + 2$ exists, then so does $(n + 2) + 1$; (or $n + 3$).

etc.

If $n + a_0$ exists, then so does $(n + a_0) + 1$ (for some value a_0 given above).

So by continuing with this process, we eventually reach the value $n+n$, or $2 \cdot n$.

At this stage, we could say that *'twice infinity is infinity'*. We could even quote another example of this by the experience of Hotel Hilbert: an infinite number of guests now arrive requiring accommodation. To achieve this, each existing guest is moved into the room number which is twice their current room number. This means that all the odd-numbered rooms are now available for the new arrivals. The falsehood is the same as before—infinity is not a number. Since it is not a number, as mathematicians we should say in preference that *if n exists, then so does the number* $2 \cdot n$.

In any case if we have the expression $2 \cdot n = n$, are we to assume that $n = \infty$? The only value to fit this is $n = 0$, a long way short of infinity.

Continuing with the counting sequences: If $2 \cdot n$ exists, then so does $2 \cdot n + 1$. This process continues and during its continuation we make the numbers $3 \cdot n$, $4 \cdot n$, $5 \cdot n$, ..., $a_1 \cdot n + a_0$ (for $0 \leq a_1 < n$), ..., until we count to $n \cdot n$, or n^2.

Cantor (Georg Ferdinand Ludwig Philip Cantor, 1845–1918) uses this situation to show that sets of such numbers are denumerable. He does this by taking two numbers j and k (where $1 \leq j, k \leq n$), and forming sets of fractions of the type j/k, arranged in a square matrix. The cardinality of this set of fractions is n^2 – inclusive of those which have a common factor in the numerator and denominator, or otherwise reduce to a common value. His arrangement here does seem to be somewhat superfluous, in that after constructing a square containing these number pairs, he then shows that a diagonal line can be drawn back and forth through each of these pairs. He could have taken any size of square, divided it into cells and then counted them to show the same result. The same is true of any size of rectangular table also. As a simple example of this, construct a square and divide it into 10 by 10 cells. Then take the number pairs, $(0,0)$, $(0,1)$, $(0,2)$, ..., $(9,9)$ and put each in a different cell. No matter how you arrange these (randomly if you wish), the end result is the same in that each cell has only one number pair as its contents, no pair of numbers is repeated and there are no empty cells. The cells in this grid could be numbered by their columns and rows such that a one-to-one mapping could be constructed between each cell's reference and each of the above number pair. The end result in all of these is to demonstrate that *if n exists, then so does* n^2. (Or in the rectangular case, the cardinality of the table is the product of two positive numbers.) To be fair about this, the diagonal line passes through all the cells and thus shows that each number pair is counted once.

We could continue the counting process, but rather than be long-winded about it, I'll take stock of the situation so far. Taking the wider view of the situation: by a process of counting we have constructed a system of addition, which leads to multiplication and then to exponentiation. I refer to this as the 'Archimedean Process'.

Thus if n exists, then so does $a_n \cdot n^n + a_{n-1} \cdot n^{n-1} + \cdots + a_1 \cdot n + a_0$ (for $0 \leq a_i < n$).

This polynomial format also indicates that any number can be expressed in any radix. Furthermore, the (Archimedean) process doesn't end with n^n; it continues with n^{n+1}, n^{n+2}, ..., n^{n+m}, etc.

It would seem that for any (positive) numbers, n and m, $0 \leq m, n$ there exists m^n. (I have swapped m with n to illustrate the next example.)

Of particular interest here is when $m = 10$, which brings me to another of Cantor's proofs.

Depending on which version you read, Cantor considers a list of *all* (decimal) numbers between 0 and 1. For the purposes of this exercise, you are led to believe that each of the numbers in this list is either irrational or never-ending in some way. From this list, he takes the first digit of the first number, the second digit from the second number, the third digit from the third number, and so on—this is Cantor's 'Diagonal Process'. Each of these digits is changed in some way and then they are placed back together (in their original decimal columns) to make a new number. He then states that this new number cannot be the same as any other number in the original list because there is at least one digit different in at least one decimal column.

I believe that Cantor may have fallen into a trap! I think he may have assumed that because there are an infinite number of rows and of columns, then the number of rows and the number of columns in his list are equal.

Returning to my above consideration of m^n, when $m = 10$. If n exists, then so does 10^n.

My strategy is to choose a number, n, and write every n-digit decimal in a list. This list has $0.000\ldots$ as its first entry and $0.999\ldots$ as its last. Any other decimal number is somewhere between these extremes. It is also the case that if I multiply each decimal in my list by 10^n, the result is the counting or indexing set of numbers (for convenience, I include 0 in the counting numbers).

For $n = 1$, $10^1 = 10$. So there are 10 1-digit numbers.

For $n = 2$, $10^2 = 100$. So there are 100 2-digit numbers. Etc.

These lists consist of n columns and 10^n rows. No matter how I choose n digits and arrange them into a decimal number, I can always find that number in my list. This can be demonstrated (if not proven by mathematical induction) as follows:

If I have a full list of decimal numbers in n columns then I could regard these numbers as a string of characters (in the computer sense of a string-variable). For each string, I can append each of the digits 0 to 9 in turn, then convert the string back to decimal format and so increase my row count ten-fold for each extra column. Another way to think of this extension of decimal places is to multiply each existing decimal by 10^{n+1}, add each of the numbers 0 to 9 to make ten new numbers and then divide these by 10^{n+1} to revert to the required decimal listing. In simple mathematical terms: $10 \cdot 10^n = 10^{n+1}$.

This indicates that if n exists, then so does the number, $n + 1$ (in the number of columns), and that if n exists, the so does 10^n and also 10^{n+1} (in the number of rows).

Another example is given in chapter 2 of *Computability and Logic* by George S. Boolos & Richard C. Jeffrey, (3rd edition, Cambridge University Press 1991, an OU set book for M335, M381, etc.). From the note (*'following Georg Cantor'*) in the text, I assume that this next process is a variation of the above diagonal process.

They consider the set of *all sets of positive integers*. This set has the empty set, the set of every positive integer and every set in between these two extremes as its subsets. They then describe a type of diagonal process in which if a certain number does not appear in a certain subset then a new set comprising of these 'missing' numbers is compiled. Then it is claimed that this new set cannot be a subset of the original set.

Looking at this situation from the Archimedean Process, it would seem to me to be a case of: if n exists, the so does 2^n.

I have a set of n items (in this case the numbers from 1 to n), from which I make subsets comprising of combinations of 1, 2, 3, ..., r items. The total number of subsets derived by combinations of r-choices from a list of n items can be seen in the nth row of Pascal's Triangle.

The sum of the entries in each row is 2^n, as I will now demonstrate. The first few rows of the Triangle have this property, so assume this of the kth row. Adjacent pairs of numbers are added together to make the $(k + 1)$th row, so that each number is added twice (with the exception of the 1s at each end which are only added once), once to its neighbour to the left, and

once to the right. Two 1s are placed, one at each end of the $(k+1)$th row so that its sum becomes 2^{k+1}. Since the Pascal's Triangle is well defined as are the associated combinations that it enumerates, I fail to see why this 'extra' set isn't a subset of the original set.

It is always difficult to challenge a long-standing principle. Has it survived all these years because nobody dared to challenge it, or is it really true? Has it merely been accepted without question? It is obvious to me that something is wrong. But I wonder if I am missing something in the argument. Have I taken a view that is too simplistic? Is my maths of sufficient standard to understand the problem (let alone to solve it)? Is there some sort of process which takes effect in the transition from finite to infinite? Even with these doubts and although this essay is presented in an informal manner, I don't think that the mathematical content is sufficiently strong to prove that Cantor was wrong about (all) non-denumerable sets.

However, I will claim that there is a contradiction between the various techniques (mostly mathematical induction) used in my arguments and Cantor's theory. I suspect that the diagonal process, although a powerful mathematical tool, is used inappropriately in the examples quoted above. I think that the use of such a process should be restricted to a tabular format (in any number of dimensions, n such that $n \geq 2$) where the count of entries in each dimension is the same, so that each $(n-1)$-dimensional surface intersects with the main diagonal. Analysis using the diagonal process within this table should be restricted to the main diagonal.

Finally, a puzzle for you to ponder: Take a finite-length line. Are the points on this line denumerable? I suggest the following will indicate that they are, even with the knowledge that between any two points on a line there are an infinite number of points.

Mark the point at one end of this line with 0 and the other end with 1, now divide the line into ten segments of equal length and so mark the points $0.1, 0.2, \ldots, 0.9$. Divide each segment into ten equal smaller segments and mark the remaining points $0.01, 0.02, \ldots, 0.99$. Divide each subsequent segment into ten and continue this process until every point is marked with a decimal number. If my reasoning is correct and the decimal numbers are denumerable then so are the points on a line.

TEACHER: "What's the largest number?"

SMALL BOY: "1,000,000,000,000,000,000,000,000,000,000."

TEACHER: "What about 1,000,000,000,000,000,000,000,000,000,001?"

SMALL BOY: "Well, I nearly got it right, didn't I?"

Solution 255.1 – Elementary trigonometry

This came up while I (TF) was investigating something to do with mutually touching finite cylinders. I must admit total disbelief initially and having to resort to a calculator to 'prove' it. Show that

$$\cot\left(\frac{\pi}{6}-\frac{1}{2}\arccos\frac{11}{14}\right) \;=\; 3\sqrt{3}. \qquad (1)$$

Ken Greatrix

I made a half-hearted attempt at the solution, in the expectation that after several hours and as many pages of scribbling, I still wouldn't have achieved anything. So, you can imagine my surprise when the answer 'popped out' after just two pages. I have therefore decided to offer my solution in its almost draft form. With this in mind, I suspect that there's an easier way to the same solution.

I started by converting the cotangent expression into its tangent:

$$\begin{aligned}\cot\theta &= \tan\left(\frac{\pi}{2}-\theta\right),\\ \cot\left(\frac{\pi}{6}-\frac{1}{2}\cos^{-1}\frac{11}{14}\right) &= \tan\left(\frac{\pi}{2}-\frac{\pi}{6}+\frac{1}{2}\cos^{-1}\frac{11}{14}\right)\\ &= \tan\left(\frac{\pi}{3}+\frac{1}{2}\cos^{-1}\frac{11}{14}\right).\end{aligned}$$

I then thought it might be easier if I changed the arccos to an arctan, with the idea that it would be cancelled by the required tangent. By applying Pythagoras's theorem, the third side of a right-angled triangle is $\sqrt{75}$, or $5\sqrt{3}$. This now has the form of a tangent of the sum of two angles.

$$\tan\left(\frac{\pi}{3}+\frac{1}{2}\tan^{-1}\frac{5\sqrt{3}}{11}\right) \;=\; \frac{\tan\frac{\pi}{3}+\tan\left(\frac{1}{2}\tan^{-1}\frac{5\sqrt{3}}{11}\right)}{1-\tan\left(\frac{\pi}{3}\right)\tan\left(\frac{1}{2}\tan^{-1}\frac{5\sqrt{3}}{11}\right)}. \qquad (*)$$

At this stage I began thinking that 'tan of arctan is' ... 'an awkward expression when $\frac{1}{2}$ is stuck in the middle of it'. Perhaps the half-angle formula might help. My books only give expressions for sine and cosine, so I combined these for the tangent. Later I looked on the internet and found the same expression:

$$\tan\frac{\theta}{2} \;=\; \sqrt{\frac{1-\cos\theta}{1+\cos\theta}}.$$

From the original expression, we know that $\cos\theta = 11/14$; so

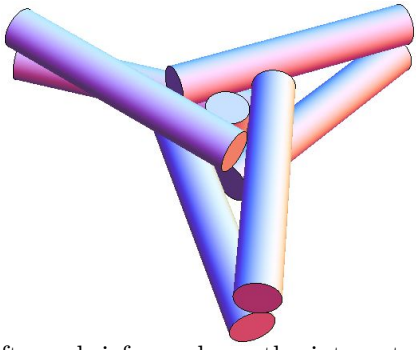
$$\tan\frac{\theta}{2} = \sqrt{\frac{1-11/14}{1+11/14}} = \frac{\sqrt{3}}{5}.$$

Since $\tan\pi/3 = \sqrt{3}$, the above expression $(*)$ simplifies to

$$\frac{\sqrt{3}+\sqrt{3}/5}{1-\sqrt{3}\cdot\sqrt{3}/5}$$

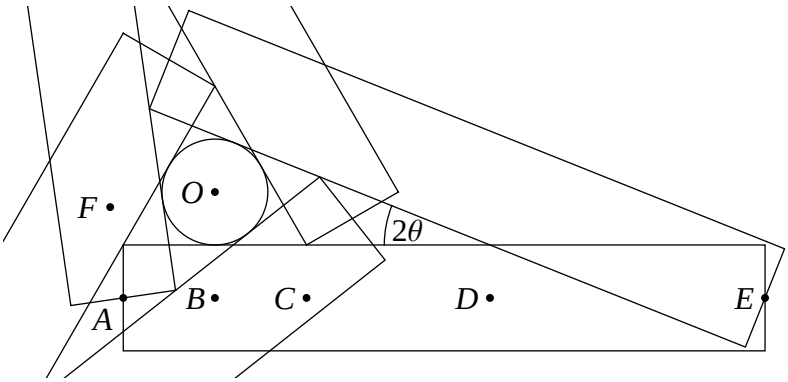
from which, after cancelling and rearranging, we get $3\sqrt{3}$ as required.

Tony Forbes



The problem concerning 'something to do with mutually touching finite cylinders' is illustrated on the right. There are seven cylinders of radius 1. A short cylinder of length 2 in the centre is surrounded by six cylinders of length d in such a manner that each makes contact with each other. What is d?

In fact $d = 7\sqrt{3}$, as I discovered after a brief search on the internet. Equality (1) on the previous page arose from my own attempt to reproduce this answer, which I shall now try to explain.



Remembering that the cylinders (most of which have become rectangles in the diagram) have radius 1, we see from the equilateral triangle surrounding the circle that $|AB| = |BC| = |AF| = \sqrt{3}$. Also from triangle OBE we

get $|BD| = |DE|$. So we want to show that $|BD| = 3\sqrt{3}$. I suspect someone will tell me this is obvious. In case it isn't we proceed as follows.

Let the two cylinders meet at angle 2θ. Then $|BD| = \cot\theta$ and to get another equation involving θ we look at quadrilateral $OFAB$. Its internal angles are $O = 60^\circ + 2\theta$, $A = 120^\circ - 2\theta$, $B = F = 90^\circ$; so, using the cosine rule, we get two expressions for the length of the diagonal FB:

$$8 - 8\cos(60^\circ + 2\theta) \;=\; |FB| \;=\; 6 - 6\cos(120^\circ - 2\theta) \;=\; 6 + 6\cos(60^\circ + 2\theta).$$

Hence $\cos(60^\circ + 2\theta) \;=\; 2/14$ and therefore

$$|BD| \;=\; \cot\theta \;=\; \cot\left(\frac{1}{2}\arccos\frac{2}{14} - \frac{\pi}{6}\right) \;=\; 3\sqrt{3}. \qquad (2)$$

Unfortunately I must have forgotten some of the details of my original analysis of the seven cylinders problem because (2) is not quite the same as (1); but at least we now have another interesting expression for $3\sqrt{3}$.

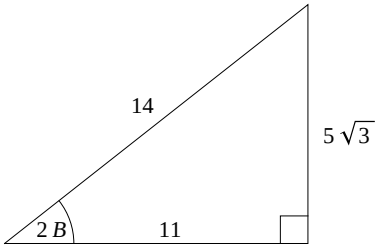
Steve Moon

We can use standard identities to write

$$\cot(A - B) \;=\; \frac{1}{\tan(A - B)} \;=\; \frac{1 + \tan A \tan B}{\tan A - \tan B}. \qquad (*)$$

Here, set $A = \pi/6$; so $\tan A = 1/\sqrt{3}$. Also set $B = 1/2\arccos(11/14)$ and assume $0 < B < \pi/2$. Hence $\cos 2B = 11/14$. Consider the triangle on the right. Then

$$\tan 2B \;=\; \frac{5\sqrt{3}}{11} \;=\; \frac{2\tan B}{1 - \tan^2 B}.$$



Hence $5\sqrt{3}\tan^2 B + 22\tan B - 5\sqrt{3} = 0$ and solving for $\tan B$ gives

$$\tan B \;=\; \frac{-22 \pm \sqrt{22^2 + 300}}{10\sqrt{3}} \;=\; \frac{6}{10\sqrt{3}} \;=\; \frac{\sqrt{3}}{5}.$$

on taking the positive root. Now substitute back into $(*)$

$$\cot\left(\frac{\pi}{6} - \frac{1}{2}\arccos\frac{11}{14}\right) \;=\; \frac{1 + 1/\sqrt{3}\cdot\sqrt{3}/5}{1/\sqrt{3} - \sqrt{3}/5} \;=\; 3\sqrt{3}.$$

Problem 257.1 – Sorting by prefix reversal

Tony Forbes

A permutation of $(1, 2, \ldots, n)$ is sorted by repeatedly reversing an initial segment. To see how this works, observe that $(1, 3, 2)$ can be sorted in three moves,

$$(\underline{1, 3}, 2) \;\to\; (\underline{3, 1, 2}) \;\to\; (\underline{2, 1}, 3) \;\to\; (1, 2, 3),$$

where to make things clear I have underlined the initial segments that are being reversed. Moreover it is not too difficult to show that three moves are always sufficient and sometimes necessary.

A problem is suggested. What is the maximum number of moves, $P(n)$, required to sort n elements by prefix reversal? Alternatively, $P(n)$ is the smallest number such that all $n!$ permutations are generated by starting from $(1, 2, \ldots, n)$ and applying up to $P(n)$ prefix reversals in all possible ways. This has also been called the *flipping pancake problem* presumably because its solution provides a convenient and efficient method of rearranging a stack of pancakes into descending order of area.

Obviously $P(1) = 0$, $P(2) = 1$, and, as we have seen, $P(3) = 3$. With a little more brute force one can compute $P(4) = 4$ and $P(5) = 5$. However, when $n = 6$ six moves generate only 718 permutations, all except $(4, 6, 2, 5, 1, 3)$ and $(5, 3, 6, 1, 4, 2)$; thus you can confirm that $P(6) = 7$. Thereafter the difficulty seems to increase very rapidly. So we suggest a possibly much easier problem for you to solve.

> Either prove that $P(n) + 1 \le P(n + 1) \le P(n) + 2$, or find a counter-example.

According to Neil Sloane's *The On-Line Encyclopedia of Integer Sequences*, the exact value of $P(n)$ is known only up to $P(17) = 19$, the $+2$ jumps occurring at $n = 3$, 6 and 11. So there is still an infinite amount of work to be done.

In the absence of a complete solution to the problem of sorting by prefix reversal one can nevertheless try to obtain a good estimate for $P(n)$. In 1978 the upper bound $P(n) \le (5n + 5)/3$ was published by W. H. Gates[1] & C. H. Papadimitriou. This has since been improved at least for large n to $P(n) \le 18n/11 + O(1)$ by B. Chitturi, W. Fahle, Z. Meng, L. Morales, C. O. Shields, I. H. Sudborough & W. Voit in 2008. It is sobering to measure thirty years of progress by comparing $18/11 \approx 1.636$ with $5/3 \approx 1.667$.

[1] Founder of a large computer software company

Solution 229.3 – Harmonic triangle

In this array of fractions

$$\begin{array}{ccccccccccc}
 & & & & & \frac{1}{1} & & & & & \\
 & & & \frac{1}{2} & & & & \frac{1}{2} & & & \\
 & & \frac{1}{3} & & & \frac{1}{6} & & & \frac{1}{3} & & \\
 & \frac{1}{4} & & \frac{1}{12} & & & & \frac{1}{12} & & \frac{1}{4} & \\
 & & & & & \cdots & & & & &
\end{array}$$

the first fraction in the n^{th} row is $1/F(n,1) = 1/n$ and the r^{th} fraction in the n^{th} row is

$$\frac{1}{F(n,r)} = \frac{1}{F(n-1,r-1)} - \frac{1}{F(n,r-1)},$$

$r = 1, 2, \ldots, n$. Find a general formula for $F(n,r)$. Hence show that each row is symmetrical about the centre.

Steve Moon

Given

$$\frac{1}{F(n,1)} = \frac{1}{n} \quad \text{and} \quad \frac{1}{F(n,r)} = \frac{1}{F(n-1,r-1)} - \frac{1}{F(n,r-1)},$$

we try to establish a pattern by computing

$$\begin{aligned}
\frac{1}{F(n,2)} &= \frac{1}{F(n-1,1)} - \frac{1}{F(n,1)} = \frac{1}{n-1} - \frac{1}{n} = \frac{1}{n(n-1)}, \\
\frac{1}{F(n,3)} &= \frac{1}{F(n-1,2)} - \frac{1}{F(n,2)} = \frac{2}{n(n-1)(n-2)}, \\
\frac{1}{F(n,4)} &= \frac{1}{F(n-1,3)} - \frac{1}{F(n,3)} = \frac{6}{n(n-1)(n-2)(n-3)}.
\end{aligned}$$

From the pattern of these results we conjecture that

$$\frac{1}{F(n,r)} = \frac{(n-r)!(r-1)!}{n!}. \qquad (*)$$

We prove this by induction. We know that the proposition is true for $r = 1$, 2, 3, 4. Assume $(*)$ is true for general $r = k$. For $r = k+1$,

$$\begin{aligned}
\frac{1}{F(n,k+1)} &= \frac{1}{F(n-1,k)} - \frac{1}{F(n,k)} \\
&= \frac{(n-k-1)!(k-1)!}{(n-1)!} - \frac{(n-k)!(k-1)!}{n!} = \frac{(n-(k+1))!k!}{n!}.
\end{aligned}$$

So if $(*)$ is true for $r = k$, it is true for $r = k + 1$; hence $(*)$ holds for $r \geq 1$.

The general expression required is

$$F(n, r) \;=\; \frac{n!}{(n-r)!(r-1)!}.$$

Furthermore by replacing r by $n - r + 1$ we get

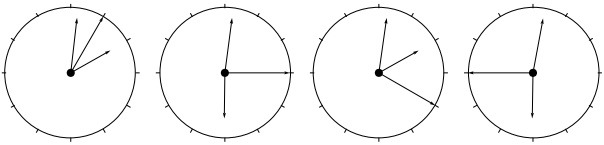
$$F(n, n-r+1) \;=\; \frac{n!}{(n-n+r-1)!(n-r+1-1)!} \;=\; F(n, r).$$

Observe, by the way, that all this works even when the second parameter exceeds n, giving $F(n, r) = 0$ for $r > n$.

Problem 257.2 – Three hands

Tony Forbes

On a standard 12-hour analogue clock, for what proportion of the day is the second hand in the smaller angle between the minute hand and the hour hand, as happens, for example, at 02:01:05 and 06:01:15 but not at 02:01:20 and 06:01:45.



Yes, I know there are times when the angle is exactly 180° (exercise for reader: when?). However, they form a null set and can therefore be ignored. And while we are on the subject, can you always tell the time even if the three hands are indistinguishable?

Problem 257.3 – Divisor sums of powers

This came up recently on the internet forum NMBRTHRY. As usual, let $\sigma(n)$ denote the sum of the divisors of n. Then $\sigma(16) = 1 + 2 + 4 + 8 + 16 = 31 = 1 + 5 + 25 = \sigma(25)$. A problem suggests itself. When does $\sigma(a^2) = \sigma(b^2)$? More generally, find solutions of $\sigma(a^k) = \sigma(b^k)$. In NMBRTHRY, Zhi-Wei Sun reported solutions with $k = 3$, including $\sigma(48142241^3) = \sigma(48374911^3)$, but I am unaware of any non-trivial examples with $k \geq 4$.

Solution 231.1 – Log 12

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

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

Steve Moon

First focus on the terms on the right-hand side in S_r:

$$\begin{aligned}
S_2 &= \frac{1}{4^2} + \frac{1}{6^2} + \frac{1}{8^2} + \frac{1}{9^2} + \frac{1}{10^2} + \frac{1}{12^2} + \ldots, \\
\frac{S_4}{2} &= \frac{1}{2}\left(\frac{1}{4^4} + \frac{1}{6^4} + \frac{1}{8^4} + \frac{1}{9^4} + \frac{1}{10^4} + \frac{1}{12^4} + \ldots\right), \\
\frac{S_6}{3} &= \frac{1}{3}\left(\frac{1}{4^6} + \frac{1}{6^6} + \frac{1}{8^6} + \frac{1}{9^6} + \frac{1}{10^6} + \frac{1}{12^6} + \ldots\right), \\
&\ldots \\
\frac{S_{2m}}{m} &= \frac{1}{m}\left(\frac{1}{4^{2m}} + \frac{1}{6^{2m}} + \frac{1}{8^{2m}} + \frac{1}{9^{2m}} + \frac{1}{10^{2m}} + \frac{1}{12^{2m}} + \ldots\right).
\end{aligned}$$

Now the first terms form an infinite sum, which is a Taylor series:

$$\frac{1}{4^2} + \frac{1}{2}\cdot\frac{1}{4^4} + \frac{1}{3}\cdot\frac{1}{4^6} + \cdots + \frac{1}{k}\cdot\frac{1}{4^{2k}} + \ldots \ = \ -\log\left(1 - \frac{1}{4^2}\right).$$

Similarly the second terms sum to $-\log(1 - 1/6^2)$ and so on. Therefore

$$\begin{aligned}
S_2 + \frac{S_4}{2} + \frac{S_6}{3} + \frac{S_8}{4} + \ldots \ &= \ -\sum_{n=4,\ n \text{ composite}}^{\infty} \log\left(1 - \frac{1}{n^2}\right) \\
&= \ \sum_{n=4,\ n \text{ composite}}^{\infty} \log\left(\frac{1}{1 - 1/n^2}\right). \qquad (1)
\end{aligned}$$

From the properties of the Riemann zeta function, $\zeta(s)$,

$$\zeta(s) \ = \ \sum_{n=1}^{\infty} \frac{1}{n^s} \ = \ \prod_{p \text{ prime}} \frac{1}{1 - 1/p^s}.$$

Therefore

$$\zeta(2) \;=\; \frac{\pi^2}{6} \;=\; \prod_{p \text{ prime}} \frac{1}{1-1/p^2},$$

$$\log\zeta(2) \;=\; 2\log\pi - \log 6 \;=\; \sum_{p \text{ prime}} \log\frac{1}{1-1/p^2}.$$

So we now have

$$\log 6 \;=\; 2\log\pi - \sum_{p \text{ prime}} \log\frac{1}{1-1/p^2}. \tag{2}$$

Also we can relate the infinite sums in (1) and (2):

$$\sum_{n=2}^{\infty} \log\frac{1}{1-1/n^2} \;=\; \sum_{p \text{ prime}} \log\frac{1}{1-1/p^2} \;+\; \sum_{n\geq 4,\ n \text{ composite}} \log\frac{1}{1-1/n^2}$$

$$=\; 2\log\pi - \log 6 + S_2 + \frac{S_4}{2} + \frac{S_6}{3} + \frac{S_8}{4} + \ldots. \tag{3}$$

Now $1/(1-1/n^2) = n/(n-1)\cdot n/(n+1)$. Hence

$$\sum_{n=2}^{\infty} \log\frac{1}{1-1/n^2} \;=\; \sum_{n=2}^{\infty} \log\frac{n}{n-1} + \sum_{n=2}^{\infty} \log\frac{n}{n+1}. \tag{4}$$

If we form a few terms on the right-hand side,

$$\log 2 + \log\frac{2}{3} + \log\frac{3}{2} + \log\frac{3}{4} + \log\frac{4}{3} + \log\frac{5}{4} + \ldots,$$

we note that $\log\big((k+1)/k\big) + \log\big(k/(k+1)\big) = 0$. So by 'telescopic cancellation' the infinite sum (4) is convergent and

$$\sum_{n=2}^{\infty} \log\frac{1}{1-1/n^2} \;=\; \log 2.$$

Hence from (3),

$$\log 2 \;=\; 2\log\pi - \log 6 + S_2 + \frac{S_4}{2} + \frac{S_6}{3} + \frac{S_8}{4} + \ldots,$$

which on rearranging becomes

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

Solution 255.3 – Points of inflexion

A *point of inflexion* occurs at (u, v) on the elliptic curve $y^2 = x^3 + ax^2 + bx + c$ if the tangent at (u, v) meets the curve at a triple point. Show that the x coordinate of a point of inflexion occurs at a root of

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2. \qquad (*)$$

Now forget about elliptic curves. Given a quartic of the form $(*)$ with real a, b and c, explain why it cannot have more than one real root u for which $u^3 + au^2 + bu + c \geq 0$ except possibly when the cubic has zero discriminant.

Steve Moon

For a point of inflection we require $d^2y/dx^2 = 0$. Differentiating

$$y^2 \;=\; x^3 + ax^2 + bx + c$$

implicitly,

$$2y\frac{dy}{dx} \;=\; 3x^2 + 2ax + b, \qquad 2\left(\frac{dy}{dx}\right)^2 + 2y\frac{d^2y}{dx^2} \;=\; 6x + 2a.$$

So

$$\begin{aligned}
\frac{d^2y}{dx^2} &= \frac{3x + a - (dy/dx)^2}{y} \\
&= \frac{1}{y}\left(3x + a - \frac{(3x^2 + 2ax + b)^2}{4y^2}\right) \\
&= \frac{2y^2(3x + a) - (3x^2 + 2ax + b)^2}{4y^3} \\
&= \frac{4(x^3 + ax^2 + bx + c)(3x + a) - (3x^2 + 2ax + b)^2}{4y^3}
\end{aligned}$$

and this is 0 for a point of inflexion. Hence we need only consider the numerator and equate it to zero. Expanding $4(x^3 + ax^2 + bx + c)(3x + a) - (3x^2 + 2ax + b)^2$ gives the criterion

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 \;=\; 0$$

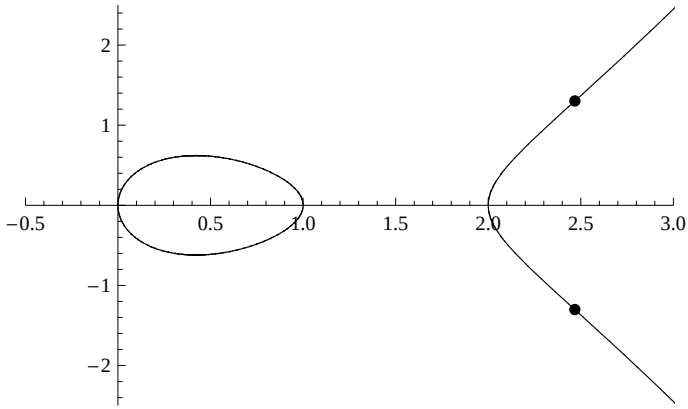
for a point of inflexion, as required.

Tony Forbes

The second part of the problem seems to be rather difficult and I have no idea how to solve it.

However, if we are allowed to cheat, by knowing that $(*)$ arises from the elliptic curve $y^2 = x^3 + ax^2 + bx + c$ (and hence the cubic $x^3 + ax^2 + bx + c$ has non-zero discriminant), there is a straightforward explanation. A point of order 3 on an elliptic curve is precisely a point of inflexion. You can see this by performing the construction described in M500 **256**, pp 6–9, or look it up in a text book such as *Rational Points on Elliptic Curves* by J. H. Silverman & J. Tate.

We now use the fact that the *real* points of order 3 on a real elliptic curve, together with the point at infinity, form a group isomorphic to $\mathbb{Z}_3$. So there must be precisely two of them, and they must occur at $(u, \pm v)$ for some root u of $(*)$ and for real $v = \sqrt{u^3 + au^2 + bu + c} > 0$. If you draw a typical elliptic curve, you can probably see where they are. For example, on $y^2 = x^3 - 3x^2 + 2$ they occur at $(2.46789, \pm 1.30191)$ approximately.



Since the relation between roots and inflexion points is reversible, this means that when a, b and c are real, $(*)$ must have precisely one real root u for which $u^3 + au^2 + bu + c$ is positive. We would be very interested if anyone can prove this directly without reference to elliptic curves.

On the other hand, it is known that the group of complex points of order 3 together with the point at infinity is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. Now there must be eight distinct points of inflexion $(u, \pm v)$, two for each of the four complex roots of $(*)$.

Problem 257.4 – Tracks

Tony Forbes

Your MP3 player has tracks, T_0, T_1, ..., T_n of lengths t_0, t_1, ..., t_n respectively. The device selects tracks at random and plays them in full. The probability of track T_i getting selected is proportional to t_i. For what fraction of the time would you expect to be listening to track T_0?

If the general problem is too difficult, try this special case instead. Suppose you have 30 minutes of music, one long track, T_0 of 20 minutes, and $n \geq 1$ short tracks of $10/n$ minutes each. So, when the MP3 player makes its selection, T_0 is chosen with probability 2/3 and each of the others with probability $1/(3n)$. I imagine you can expect to be listening to T_0 quite often, but for what fraction of the time I unfortunately cannot say, except that it is significantly greater than 2/3.

Problem 257.5 – The diameter graph

Take a set S of n points in the plane. Construct G, the *diameter* graph of S, as follows. Vertices of G are the points of S. If A and B are vertices, then $\{A, B\}$ is an edge of G if $|A - B|$, the Euclidean distance between points A and B, is the maximum over all pairs of points in S. Prove that G contains no cycle of even length.

For example, if the points form an equilateral triangle, every distance between a pair is of maximum length, and hence G is the triangle graph, K_3, which indeed has no even cycles. On the other hand, if the points of S form a square, the graph consists of two disjoint components each with two vertices joined by an edge and, again, it is even cycle free.

The problem was described in an article by Filip Morić & János Pach — Two and a Half Billion Years of Distance Research, *Geombinatorics* **XXII**, April 2013, Celebrating the Centenary of Paul Erdős' Birth — where they say it appeared in the problem section of *Jahresbericht der Deutschen Mathematiker–Vereinigung* **43** (1934), posed by Heinz Hopf and Erika Pannwitz.

The 'Two and a Half Billion Years' refers to Erdős's estimate of his own age. In his youth the Earth was known to be approximately two billion years old. However, by the time Erdős reached old age the figure had increased to something nearer 4.5 billion.

Fermat's Last Theorem and Pythagorean triples

Peter L. Griffiths

The quadratic equation difference consists of one term $4pq$ calculated as follows: $(p+q)^2-(p-q)^2 = 4pq$, where p and q are integers. This one term $4pq$ has an integer square root if p and q both have integer square roots. This does not apply if the power n is an integer higher than 2, where there will always be two terms or more.

The cubic equation difference consists of two terms $6p^2q + 2q^3$; that is,

$$(p+q)^3-(p-q)^3 = (p^3+3p^2q+3pq^2+q^3)-(p^3-3p^2q+3pq^2-q^3) = 6p^2q+2q^3.$$

If the alternating series is omitted, we have $p^3 + 3p^2q + 3pq^2 + q^3$ comp $6p^2q + 2q^3$. If $p = q$, then these two expressions will be equal, that is $p^3 + 3p^3 + 3p^3 + p^3 = 6p^3 + 2p^3$. This equality when $p = q$ applies to all the powers. But $8p^3$ clearly has an integer cube root, whereas $6p^2q+2q^3$ at first sight does not have an integer cube root unless $p = q$. Can $6p^2q + 2q^3$ have an integer cube root without p equalling q?

Assume $p > q$, so that $q = p/r$, where r is equal to or greater than 1. Then $6p^2q + 2q^3$ can be expressed as $6p^2p/r + 2(p/r)^3$; this equals $p^3(6/r + 2/r^3)$. The number $r = p/q$ must be rational, but the cube root of $6/r+2/r^3$ is almost certainly irrational unless $r = 1$; that is, $(6r^2 + 2)^{1/3}$ is almost certainly irrational unless $r = 1$; that is unless $p = q$.

More generally, for the integer nth root greater than 2, the nth root of

$$2\left(\binom{n}{1}r^{n-1} + \binom{n}{3}r^{n-3} + \binom{n}{5}r^{n-5} + \dots\right)$$

will be irrational unless $r = 1$. The product $2 \times 2^{n-1}$ will always have 2 as the nth root. Where n is an integer other than 1, the real nth root of 2 is always an irrational number special to that particular value of n. It likewise follows that the $(1 - 1/n)$ root of 2 is also irrational but this corrects the irrationality of $2^{1/n}$.

In the FLT case under examination, $2^{1/n}$ always remains unchanged, but in the event of r exceeding 1, $2^{1-1/n}$ will change and will cease to correct the irrationality of $2^{1/n}$, which will persist uncorrected. This is the factorial mathematical explanation and proof of Fermat's Last Theorem. It is a matter of distinguishing rational from irrational amounts, and the correction of irrationality.

Erratum In M500 **255**, '$3x^2 = (z + x)(z - y)$' on page 6, line −6 should read '$3x^2 = (z + y)(z - y)$'.

Contents M500 257 – April 2014

04.00

Front cover Five hundred random clocks. Those coloured grey (cyan) have the second hand between the hour and minute hands. See page 15.