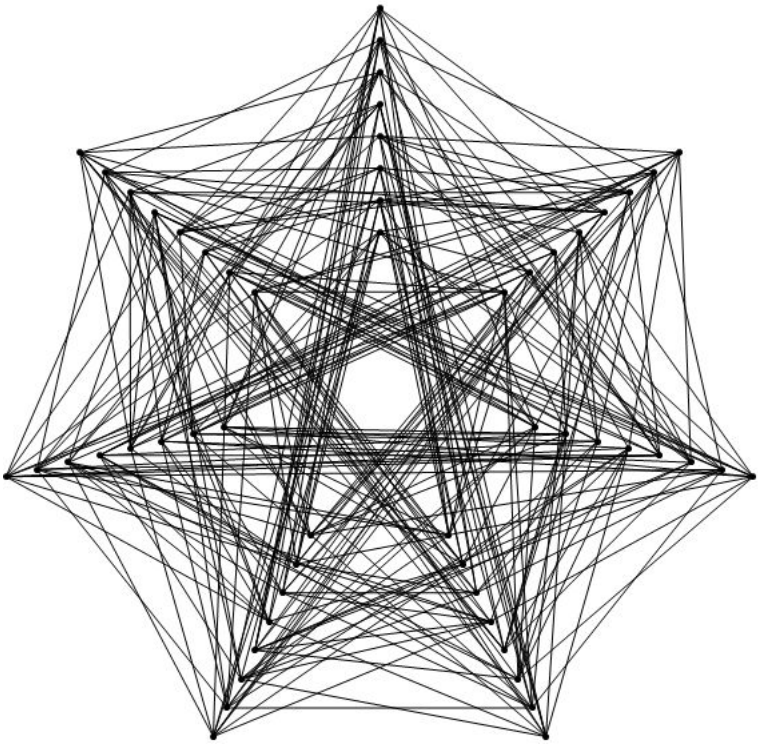
*

ISSN 1350-8539

M500

M500 228



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.

Integer logarithms on finite fields

Tommy Moorhouse

Introduction In other articles we have considered integer logarithms of the natural numbers. It seems natural to ask whether integer logarithms exist for finite fields and, if so, to explore their properties. In fact these logarithms do exist and in some cases form the basis of the 'index calculus' [Apostol]. In the circumstances below they are group isomorphisms and have inverses, and we use these to construct and explore what is known as a group action.

Readers who know something about groups (and those who don't but are willing to do some simple checking) should have no trouble understanding, and hopefully enjoying, this article. All the terms will be explained as they are introduced, but basic properties will be used without detailed explanation. For facts about fields and so on I have included some useful introductory books in the list of references at the end of the article.

Preliminary results Our first result is something of a negative one.

Theorem 1 There is no non-trivial integer logarithm function from a finite field $\mathbb{F}$ into the same field.

Proof The number of elements of a finite field $\mathbb{F}$ is a power of a prime number, say p^α. Thus there is at least one element, say g, of the multiplicative group $\mathbb{F}^*$ of non-zero elements of $\mathbb{F}$ such that every element of $\mathbb{F}$ is a power of g. Such an element is called a generator of $\mathbb{F}^*$. For any logarithm L we must have $L(1) \equiv 0 \pmod{p^\alpha}$, since $L(n) = L(1n) = L(1) + L(n)$. Now $g^{p-1} \equiv 1 \pmod{p^\alpha}$ and so $L(g^{p-1}) \equiv (p-1)L(g) \equiv 0 \pmod{p^\alpha}$. Thus $L(g) \equiv 0$ and since every element of $\mathbb{F}$ can be expressed as g^r for some r we see that $L(a) \equiv 0 \pmod{p^\alpha}$ for all $a \in \mathbb{F}$.

The reason for the nonexistence of logarithms into the same field gives us a clue for proceeding. Given a field we can obtain any non-zero element uniquely as a power of a generator. For example, if we take the field with five elements (which is isomorphic to $\mathbb{Z}_5$ with the usual modular addition and multiplication) the powers of 2 are $2^0 = 1, 2^1 = 2, 2^2 = 4$ and $2^3 = 3$. We define $L_2(2^n) = n$, with L_2 taking values in the additive group $(\mathbb{Z}_4, +)$. For future reference we note that, although $(\mathbb{Z}_4, +)$ is a group and not a field, there is also a field of order 4.

Definitions We now proceed to define logarithms on certain fields. Initially we will be concerned with the fields of order p where p is a prime number and $p = 2^r + 1$ for some r. In the general case the fields can have order p^n for any $n > 0$, and the reader is encouraged to consider how the results below can be generalized. A good model for the more general case is the field of order 9 with elements $0, 1, 2, \alpha, 1+\alpha, 2+\alpha, 2\alpha, 1+2\alpha, 2+2\alpha$, where $\alpha^2 = 2$. Note that in general generators are not the same as primitive roots modulo p^n, because fields have elements that are not ordinary integers. In the case $n = 1$, however, the generators are just the primitive roots.

We return to the specific case introduced above, because it gives us some concrete examples. Given a field of order p as above we denote its multiplicative group by $\mathbb{GF}(p)^*$. We denote the additive subgroup $(\mathbb{Z}_{2^r}, +)$ by $\mathbb{Z}_{2^r}$. For any generator g of the multiplicative group of the field we denote the logarithm with respect to g of any element $n \in \mathbb{GF}(p)^*$ by $L_g(n)$. This lies in $\mathbb{Z}_{2^r}$. The logarithm is a group isomorphism, which essentially means that it maps one group to another having the same structure.

We denote the pre-image under L_g of any $m \in \mathbb{Z}_{2^r}$ by $E_g(m) = g^m$, lying in $\mathbb{GF}(p)^*$. By definition $L_g(E_g(m)) = m$. The letter E is supposed to suggest 'exponential': we avoid the use of 'exp' so as not to clash with the notation of Apostol.

Now for any two generators g and g' we have a sequence of maps

$$\mathbb{Z}_{2^r} \overset{E_g}{\longrightarrow} \mathbb{GF}(p)^* \overset{L_{g'}}{\longrightarrow} \mathbb{Z}_{2^r}.$$

This sequence permutes the elements of $\mathbb{Z}_{2^r}$ and is, in fact, an automorphism. This means that it maps $\mathbb{Z}_{2^r}$ to itself in a way that preserves the group structure. We call this automorphism $\sigma_{g,g'}$ or, more suggestively, $\langle g'|g\rangle$. Let us establish some properties of this group.

Theorem 2 The maps $\sigma_{g,g'} = L_{g'} \circ E_g$ are automorphisms of $\mathbb{Z}_{2^r}$.

Proof We have for elements a and b of $\mathbb{Z}_{2^r}$

$$\begin{aligned}
\sigma_{g,g'}(a+b) &= L_{g'}(E_g(a+b)) \\
&= L_{g'}(E_g(a)E_g(b)) \\
&= L_{g'}(E_g(a)) + L_{g'}(E_g(b)) \\
&= \sigma_{g,g'}(a) + \sigma_{g,g'}(b).
\end{aligned}$$

It is easily checked that the kernel of $\sigma_{g,g'}$ is the zero element of $\mathbb{Z}_{2^r}$, so that $\sigma_{g,g'}$ is indeed a group automorphism.

Not all these automorphisms are distinct. In fact we will prove that there are exactly $\phi(2^r) = 2^{r-1}$ of them in this case. We start with some lemmas.

Lemma 3 If g and g' are generators of $\mathbb{GF}(2^r+1)^*$ where 2^r+1 is prime, then $L_g(g')$ is odd.

Proof Since g' generates $\mathbb{GF}(p)^*$ multiplicatively it follows that $L_g(g')$ generates $\mathbb{Z}_{2^r}$ additively and is therefore odd.

Lemma 4 For any $a \in \mathbb{Z}_{2^r}$ we have $\sigma_{g,g'}(a) = L_{g'}(g)a$.

Proof We have

$$\begin{aligned} \sigma_{g,g'}(a) &= L_{g'}(E_g(a)) \\ &= L_{g'}(g^a) \\ &= aL_{g'}(g). \end{aligned}$$

We thus see that the automorphisms induced by our logarithms are just the action of multiplication by an odd number modulo 2^r. The set of odd numbers under multiplication modulo 2^r is a group (which we shall call $\mathcal{O}_{2^r}$), and we have what is known as a group action of $\mathcal{O}_{2^r}$ on the additive group $\mathbb{Z}_{2^r}$. Some further properties of the group can be derived. For example:

Lemma 5 $\sigma_{h,g} \circ \sigma_{k,h} = \sigma_{k,g}$.

Proof From the definitions

$$\sigma_{h,g} \circ \sigma_{k,h}(m) \;=\; L_g(E_h(L_h(E_k(m)))) \;=\; L_g(E_k(m)) \;=\; \sigma_{k,g}(m).$$

In our alternative notation we have

$$\langle g|h\rangle\langle h|k\rangle \;=\; \langle g|k\rangle.$$

Examples We return to the simple example of $\mathbb{GF}(5)^*$ with logarithms $L_2(1) = 0, L_2(2) = 1, L_2(3) = 3, L_2(4) = 2$ and $L_3(1) = 0, L_3(2) = 3, L_3(3) = 1, L_3(4) = 2$. We find that $\sigma_{2,3}(0) = 0, \sigma_{2,3}(1) = 3, \sigma_{2,3}(2) = 2, \sigma_{2,3}(3) = 1$. This is multiplication by 3 (mod 4). The group of automorphisms is the (unique) group with two elements.

The next example of this type is $\mathbb{GF}(17)^*$. The details are a little more messy but the conclusion is the same: namely that the automorphisms generated by the logarithms correspond to the multiplicative group of odd

numbers modulo 16. In our limited considerations so far the only powers of 2 leading to this situation give rise to the Fermat primes [Burton]. However, we have other possibilities.

Other fields As mentioned above there is a (unique) field with 2^n elements for any positive integer n. Note that this is not just the set $\mathbb{Z}_{2^n}$ with the usual modular addition and multiplication. To get an explicit representation of the field $GF(4)$ consider the equation $t^2 + t + 1 = 0$ over $\mathbb{Z}_2$. There are no solutions in $\mathbb{Z}_2$ (try substituting 0 and 1 into the equation and reducing modulo 2). We can add a solution, say α, to $\mathbb{Z}_2$ and form all the possible sums and multiples to get a field with four elements: 0, 1, α and $1+\alpha$. For example $\alpha(1+\alpha) = \alpha + \alpha^2 = \alpha + \alpha + 1 = 1$ using the equation satisfied by α and working modulo 2 so that $\alpha + \alpha = 0$. Now $\alpha^2 = 1 + \alpha$, $\alpha^3 = 1$, so α generates $\mathbb{GF}(4)$ and we can define our logarithms. Here $1 + \alpha$ also generates the group, so all the machinery used above can be used. The induced automorphism group acting on $\mathbb{Z}_3$ is multiplication by 2.

The key point here is that in the case of fields of non-prime order we cannot generate the whole multiplicative group from ordinary (sometimes called 'rational') integers, but we can still define logarithms by means of the generators. This gets us around the fact that there are no primitive roots modulo 2^n for $n > 1$, for example.

We will refer to logarithms formed from generators as 'basic logarithms'. It is readily seen that the sum of two logarithms is again a logarithm, that is,

$$(L_g + L_{g'})(1) \;=\; L_g(1) + L_{g'}(1) \;=\; 0 + 0 \;=\; 0$$

and

$$\begin{aligned}(L_g + L_{g'})(nm) &= L_g(nm) + L_{g'}(nm)\\ &= L_g(n) + L_g(m) + L_{g'}(n) + L_{g'}(m)\\ &= (L_g + L_{g'})(n) + (L_g + L_{g'})(m).\end{aligned}$$

However, these derived logarithms may not be basic, and indeed include the 'zero logarithm' $L_0(n) = 0$ among others.

Added interest arises from the fact that in some cases $2^n - 1$ is prime. Since $\mathbb{GF}(2^n)^*$ is generated by at least one element (not an integer) we can define the logarithm of any field element as above. The multiplicative group induced by the primitive logarithms is easily found to be the action by multiplication of the group of residue classes modulo $2^n - 1$ on the additive group $\mathbb{Z}_{2^n-1}$. In this case every non-trivial element of $\mathbb{GF}(2^n)^*$ is a generator. Readers might like to test the following conjecture.

Conjecture Given any field $\mathbb{F}$ of order p^n, the set of maps obtained from the set of basic logarithms defined for each generator by composition with the inverse ('exponential') maps in every combination give rise to a group action of the group of residue classes modulo $p^n - 1$ on $(\mathbb{Z}_{p^n-1}, +)$, the action being that of multiplication. There are $\phi(p^n - 1)$ basic logarithms and $\phi(p^n - 1)$ elements in the group acting on $(\mathbb{Z}_{p^n-1}, +)$.

A straightforward proof could involve considering the isomorphism between the multiplicative and additive groups, and mapping the generators of the additive group onto those of the multiplicative group. This suggests a method for obtaining all generators of a field $\mathbb{GF}(p^n)$ from a single generator g. First write out the powers of the generator g to find the logarithm L_g of each element. Next identify the elements a_i of the reduced residue system modulo $p^n - 1$. Finally obtain all the generators of $\mathbb{GF}(p^n)^*$ from the map $E_g(a_i) = g_i$ (that is, looking up the element of $\mathbb{GF}(p^n)^*$ that maps to a_i under L_g).

Challenge Readers who know something of group cohomology might like to see what $H^0(G, M)$ and $H^1(G, M)$ look like in the above case.

Useful books

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1998.

[2] I. Stewart, *Galois Theory*, Chapman & Hall, 1973.

[3] D. M. Burton, *Elementary Number Theory*, McGraw–Hill, 1997.

[4] S. Lang, *Algebra*, Springer, 2002,

Problem 228.1 – Odd expression

Tony Forbes

Show that the expression

$$\left\lfloor \left(3 + \sqrt{5}\right)^n \right\rfloor$$

is odd for non-negative integer n. The notation $\lfloor x \rfloor$ means the *integer part* of x; that is, the largest integer which is less than or equal to x. Previously I would have written $[x]$ for this function but nowadays the 'floor' brackets are more fashionable, and often used alongside or at least near the 'ceiling' brackets, which denote the integer you get by going the other way: $\lceil x \rceil$ is the smallest integer which is greater than or equal to x.

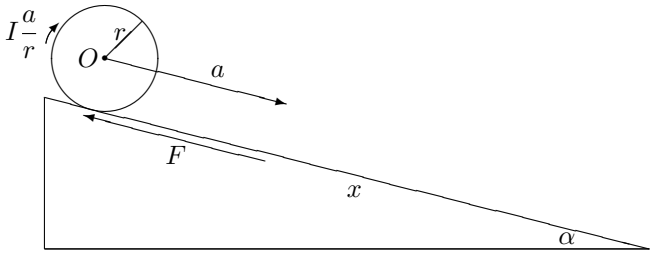
Algebra is nothing more than glorified clerking. **G. H. Hardy**

Solution 224.1 – Three rolling spheres

If the times to roll down an inclined plane are t_1 for a hollow sphere, t_2 for a solid sphere and t_3 for a 'semi-solid' sphere (solid except for a central hole of half the radius), prove that

$$t_1 : t_2 : t_3 \;=\; \sqrt{\frac{5}{3}} : \sqrt{\frac{7}{5}} : \sqrt{\frac{101}{70}} \;\approx\; 1.291 : 1.183 : 1.201.$$

Basil Thompson



Referring to the diagram above, r is the radius of the sphere, m is its mass, I is its moment of inertia, ma is the resultant force through O down the slope, and F is the friction force acting up the slope.

The sphere obeys the equations of motion

$$mg\sin\alpha - F \;=\; ma, \qquad Fr \;=\; I\,\frac{a}{r}.$$

Thus

$$mg\sin\alpha - \frac{Ia}{r^2} \;=\; ma$$

and hence

$$a \;=\; \frac{mg\sin\alpha}{m + I/r^2}. \tag{1}$$

The distance travelled is $x = \frac{1}{2}at^2$, giving

$$t^2 \;=\; 2x/a. \tag{2}$$

Using subscripts 1, 2, 3 for the three cases, we have the following values for the moments of inertia:

$$I_1 \;=\; \frac{2}{3}\,m_1r^2, \qquad I_2 \;=\; \frac{2}{5}\,m_2r^2, \qquad I_3 \;=\; \frac{31}{70}\,m_3r^3.$$

The first two are to be found in most dynamics text books. The third one is rarely quoted—I derive it at the end.

Hollow sphere From (1) we have

$$a_1 \;=\; \frac{m_1 g\sin\alpha}{m_1 + I_1/r^2} \;=\; \frac{g\sin\alpha}{1+2/3} \;=\; \frac{3}{5}\,g\sin\alpha,$$

and substituting this into (2) gives

$$t_1^2 \;=\; \frac{5}{3}\,\frac{2x}{g\sin\alpha}.$$

Solid sphere Similarly,

$$a_2 \;=\; \frac{m_2 g\sin\alpha}{m_2 + I_2/r^2} \;=\; \frac{g\sin\alpha}{1+2/5} \;=\; \frac{5}{7}\,g\sin\alpha,$$

$$t_2^2 \;=\; \frac{7}{5}\,\frac{2x}{g\sin\alpha}.$$

Half-solid sphere Again,

$$a_3 \;=\; \frac{m_3 g\sin\alpha}{m_3 + I_3/r^2} \;=\; \frac{g\sin\alpha}{1+31/70} \;=\; \frac{70}{101}\,g\sin\alpha,$$

$$t_3^2 \;=\; \frac{101}{70}\,\frac{2x}{g\sin\alpha}.$$

Hence the times t_1, t_2, t_3 are in the ratios $\sqrt{\frac{5}{3}} : \sqrt{\frac{7}{5}} : \sqrt{\frac{101}{70}}$, as stated

---

I conclude with a derivation of I_3, the moment of inertia of a half-solid sphere of radius r. This could be done by integration but is is possibly easier to take the moment of inertia of a solid sphere and subtract the moment of inertia of a solid sphere of half the radius.

Let m_3 be the mass of the half-solid sphere. Then the mass of a solid sphere of radius r made out of the same material is $\frac{8}{7}m_3$ and the mass of a solid sphere of radius $\frac{1}{2}r$ is $\frac{1}{7}m_3$. So, using the formula $I = \frac{2}{5}mr^2$ for the moment of inertia of a solid sphere, we have

$$I_3 \;=\; \frac{2}{5}\cdot\frac{8}{7}\,m_3 r^2 - \frac{2}{5}\cdot\frac{1}{7}\,m_3\left(\frac{r}{2}\right)^2 \;=\; \frac{31}{70}\,m_3 r^2.$$

Sophie's Diary: A Historical Fiction

by Dora Musielak

Eddie Kent

Some time ago I was asked to review this book for M500. Since I had recently (M500 **211 16**) noticed the film *Proof* I began reading with enthusiasm. Then I hit a snag—the book was dreadful. The style was convoluted and pretty well unreadable, the grammar was alien and the spelling was at best creative. I liked Sophie and was fascinated by what she did, but felt there was no way I could induce anyone to pay money for this. Of course being a moral coward I couldn't possibly say so, and thus I put the book aside for later consideration.

The other day I dug it out for another look, but first I checked on Amazon if it is still available. It is, but more—it is transformed. You know how they sometimes let you look at random pages? Well, it was clear that someone has done an amazing job of editing to allow the essential story to shine through. I can now say that no student of mathematics should be without it.

Pythagoras's theorem leads to one of the best understood equations in mathematics, that is, $x^2 + y^2 = z^2$. There are countless whole-number solutions to this equation and famously (apocryphally) Fermat declared that this is the case only for the number 2. He never wrote his proof of this down and callously died before he could, so the challenge became to prove 'Fermat's Last Theorem.' By the time Sophie Germain was born in April 1776 proofs had been found in a couple of special cases of $x^n + y^n = z^n$, namely $n = 3$ and 4, but the impetus to tackle the infinity-minus-two ns that remained was dying out.

Sophie's father was a merchant, financially successful but not in the top social class. If he had been things might have been easier. Although aristocratic women were not actively encouraged to study mathematics, they were expected to have sufficient knowledge of the subject to be able to discuss the topic should it arise during polite conversation. In fact books existed for this purpose. Francesco Algarotti's *Sir Isaac Newton's Philosophy Explain'd for the Use of Ladies* takes the line that women are only interested in romance, thus he explains Newton's discoveries through the flirtatious dialogue between a Marquise and her interlocutor. The teacher outlines the inverse square law of gravitational attraction, whereupon the Marquise gives her own interpretation on this fundamental law. "I cannot help thinking ... that this proportion in the squares of the distances of places ... is observed even in love. Thus after eight days absence, love becomes sixty-four times less than it was the first day."

I tell this for your amusement only, not to imply that this genre of books was responsible for inspiring Sophie Germain's interest. That life-changing

event occurred one day when she was browsing in her father's library and chanced upon Jean-Étienne Montucla's *History of Mathematics*. The chapter that caught her imagination was an essay on the life of Archimedes. The account of his discoveries was interesting enough, but what particularly kindled her fascination was the story of his death. She decided that if someone could be so consumed by a problem in mathematics that it could lead to his death, then mathematics must be a most captivating subject indeed.

So, at the age of 13, she set about teaching herself the basics of number theory and calculus (of course having to learn Latin first, word by word), and soon she was working late into the night studying the works of Euler and Newton. But this interest in such an unfeminine subject drove her mother quite frantic, and her parents tried desperately to deter her. A friend of the family, Count Guglielmo Libri-Carrucci dalla Sommaja, wrote how Sophie's father confiscated her candles and clothes and removed any heating in order to discourage her. Another blow was that the Church was banned from functioning at this period, and so she couldn't go to the nuns for help with her Latin.

Sophie's Diary is of course fictional, but it is solidly researched. As each aspect of mathematics is mastered by Sophie it is described in detail, and thus the book is dripping with equations, so it would be difficult to recommend to an average 13-year-old girl, and some kind of mathematical maturity is needed to enjoy it fully. The first equation she encounters is the above $x^2 + y^2 = z^2$; later she comes upon π and makes various approximations, and becomes adept at solving linear equations. Most importantly she realises the value of proof. Her first major setback is at $x^3 + 1 = 0$. It is clear that -1 is a solution but she knows that a cubic must have three. What can the others be?

As this is a diary, other events in the lives of ordinary people during a revolution are described. There is a nice account of the Storming of the Bastille, for instance, with its governor the Marquise de Launay having his throat cut on the steps and his head paraded through the streets. And endless meetings and discussions, her father being a deputy who had no objection to little Sophie tagging along. So apart from being a fascinating account of a person and a period, the book is also educational and an inspiration. And the point about FLT above? Well, Sophie came close to cracking it (see M500 **211** 17 for an account of Sophie Germaine's theorem).

Although she was not taken seriously as a mathematician because of her sex (having to call herself M LeBlanc) she did persevere, and was eventually accepted by some notable men, not excluding Gauss himself; she now has a street in Paris all of her own.

Buy the book; but do make sure you get the edited version (and encourage your 13-year-old daughter to read it).

The affine transformation

Dick Boardman

The affine transformation maps a point (x, y) in one plane onto the point (X, Y) in another plane. The equations are

$$X = ax + by + c, \qquad Y = dx + ey + f, \qquad ae - bd \neq 0.$$

The great virtue of the transformation is that it allows you to generalize certain results which you only need to prove in one special case. Under this transformation

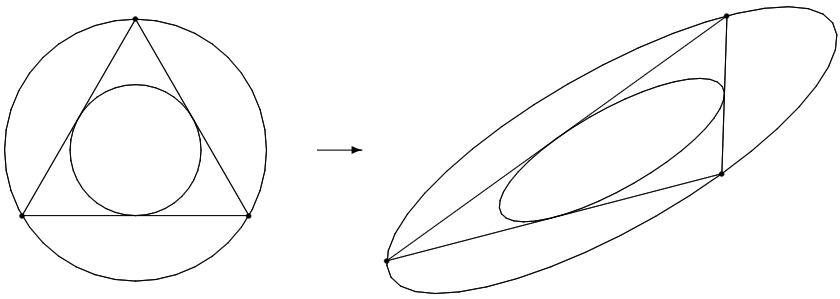
- straight lines become straight lines,
- parallel lines become parallel lines,
- ellipses and circles become ellipses and circles,
- parabolas become parabolas,
- hyperbolas become hyperbolas,
- points at infinity become points at infinity,
- ratios of lengths on the same, or parallel line segments are preserved,
- points of intersection and tangent properties are preserved.

There are six parameters which can be determined by six equations, so that three (non-collinear) points can be transformed into any other three points; that is, any triangle may be transformed into any other triangle. Some triangle properties, the intersection of the medians, for example, which depend on the mid-points of the sides, are preserved but others, like the in-centre, or the intersection of the altitudes, which depend on angle, are not. The centre of a circle becomes the centre of an ellipse. In general, angles and the ratios of line lengths on non-parallel lines are not.

Two congruent triangles with parallel sides become two congruent triangles so that two identical squares in different positions become two congruent parallelograms. From this it follows that the ratios of areas are preserved since any area filled with tiny squares will become an area filled with the same number of tiny parallelograms.

This leads to some interesting results. For example, imagine an equilateral triangle with its in-circle. This is clearly the largest ellipse which could be inscribed in that triangle. If we now transform this into any other triangle, the result will be an ellipse in a triangle. This ellipse will be the largest that could be inscribed in that triangle. The ratio of its area to that of the triangle will be the same as the ratio of the area of the in-circle to that of its equilateral triangle. Furthermore, it will touch the sides at their midpoints and its centre will be the intersection of the medians. The circle

through the vertices of an equilateral triangle will clearly be the smallest ellipse through those points. This will transform into any other triangle and the smallest ellipse surrounding it. Furthermore the centre of this smallest ellipse will be the intersection of the medians.



Continuous curves transform into continuous curves, so that a cubic curve will transform into another cubic curve with the same topology.

If the coefficients a through f are rational, then rational points will transform into rational points so that a cubic with a limited number of rational points will transform into another cubic with similar limitations. Transformations can be translations, rotations, reflections and expansions. The amount of expansion can be different in different directions.

Parameters c and f control translations. The origin in the input plane $(0, 0)$ becomes (c, f) in the output plane. Pure rotations have the form

$$X = x\cos t + y\sin t, \qquad Y = -x\sin t + y\cos x.$$

In a pure rotation there is exactly one point which is unaltered.

A pure reflection in the y-axis would be

$$X = -x, \qquad Y = y.$$

In a pure reflection there is a line of unaltered points.

The set of all possible affine transformations forms a group. This means that affine transformations have four properties.

• If two transformation are applied, one after the other, the result is an affine transformation (closure).

• If there are three affine transformations A, B and C, then (A followed by B) followed by C is the same as A followed by (B followed by C) (associative law).

- There is an identity transformation.
- Each transformation has a unique inverse.

However, A followed by B is not necessarily the same as B followed A. When A is followed by B the result may be found by using the laws for 2-dimensional matrix multiplication and addition.

In summary, the affine transformation is a restricted form of the more general projective transformation. Indeed, any of the theorems of projective geometry will also apply to the affine transformation.

Relativity without c

Sebastian Hayes

I bring to the notice of all readers interested in relativity the fascinating article Shedding Light by Mark Buchanan in the *New Scientist*, 1 November 2008. Here, the author summarizes papers by Feigenbaum and others which claim that the various space/time anomalies of Special Relativity can be deduced directly from the Galilean Relativity Principle ('That the laws of physics take the same form in all inertial frames') without assuming the invariance of the speed of light. They emerge from 'even more basic, purely mathematical considerations'. This, incidentally, allows us to attribute a small mass to the photon (and other supposed 'massless' particles). I argued in an article in the *Journal of the Open Society for Science and Technology* over twenty five years ago that the idea of a massless particle is a contradiction in terms, and by no means a necessary deduction from experiments—all we can conclude from the data is that a photon's mass would need to be smaller than 10^{-49} grams.

According to this new approach, the celebrated space/time anomalies can be deduced from consideration of certain 'rotations' and an overall space–time curvature which does not depend on the mass/energy distribution in the universe. 'Allow them [these rotations] and the mangled space-time of Einstein's relativity emerges, complete with a definite but unspecified maximum speed that the sum of individual relative speeds cannot exceed' (Buchanan, *NS* article). Buchanan quotes Feigenbaum as saying that 'these rotations ... are the wellspring of physics'. Apparently, Feigenbaum's paper has not yet been peer-reviewed but can be downloaded from www.arxiv.org/abs/0806.1234).

Summation convention, n. A mathematicians' shindig held each year in the Kronecker Delta. [Sent by JRH]

Re: Mathematics in the kitchen – V

> Recall that you were instructed to take a large, heavy, circular saucepan lid, hold it right-way up but at an angle of about 30 degrees to the horizontal, give it a spin, let it drop onto the kitchen worktop and observe its behaviour. After some ungainly spinning/rolling motion the lid reverses its direction and settles down to a steady slow rotation on which is superimposed a vibration component. As gravity exerts its influence, the vibration amplitude decreases but its frequency increases. Eventually a noisy climax is reached and the saucepan lid comes to a sudden halt.

Ken Greatrix

First of all, try it with a 2p coin on a smooth, flat, hard surface—such as a piece of glass.

It's much quieter and you get the same result. And if you do this in the kitchen, it will then fit the theme of the exercise!

If you roll the coin along, it starts to go into a curve, the radius of which gets smaller and smaller until it 'falls over'. At this point, it's going round in a circle, but this has a diameter slightly smaller than the coin. The coin itself is moving like an epicyclic gear and so will appear to be revolving backwards; as observed with the saucepan lid. As the angle to the horizontal becomes smaller, this diameter increases until it becomes the same size as the coin's—at which point motion has stopped. I suggest that it's this circular path being smaller than the diameter of the coin which causes the appearance of 'backwards' rotation.

I tried another similar experiment: Stand the coin on edge and hold it lightly with the left hand, then give it a deft flick with the right hand at its right-hand edge.

It is then spinning around a vertical diametrical axis. Unless you give it a 'perfect' flick, it will also be orbiting. Again, when it gets to a certain point it begins its 'falling-down' process. Perhaps because the edge of a 2p coin is square, it's probably impossible for it not to follow this 'orbiting' path, but while it is doing this I think it might also be turning on a very small radius circle. I tried looking at the revolving face of the coin to see if it appeared to rotate but I couldn't detect any such rotation. Perhaps this is because the light wasn't good enough and also because I couldn't maintain the spin for long enough.

Overall, it is obvious that energy in the system manifests itself in various ways (angular momentum, oscillation, kinetic energy, etc.), but I wouldn't like to attempt to model them.

Letters

How to solve quadratics

Dear Tony,

Re: M500 **223** page 15, How to solve quadratics. In *Countdown To Mathematics* Volume 3 by Lynn Graham and Dave Sargent (page 93) there is a shortcut to solving quadratic equations ax^2+bx+c where the coefficient of x^2 is greater than 1, which saves working it out by trial and error.

Example: $6x^2 - 11x - 10 = 0$.

(1) Multiply a by c: $6 \times -10 = -60$.
(2) Find two numbers whose sum is b and whose product is ac: $(-15, 4)$.
(3) Pair up those two numbers with the coefficient a: $(6, -15)$, $(6, 4)$.
(4) Factorize: $3(2, -5)$, $2(3, 2)$.
(5) Discard the common factors: $(2, -5)$, $(3, 2)$.
(6) We can now write down the factors: $(2x - 5)(3x + 2) = 0$.

So $x = 5/2$ or $-2/3$.

Keith Drever

Toroidal planets

Dear Eddie,

Thoughts on Problem 225.1 – Toroidal planet. Remember that included in the definition of a planet (which has recently been revised so as to exclude Pluto) is the stipulation that it should be large enough for its own gravity to collapse it into a sphere, or at least a spheroid.

So the answer is that if this planet-sized torus were to spring into existence, and were not revolving fast enough to keep its form, and you were standing on its inner rim, you would travel towards the centre followed at once by large amounts of rock as the thing adjusted its shape to the usual form.

There is a rather good 1960s science fiction book, *Mission of Gravity* by Hal Clements, in which humans visit a very large, very fast spinning planet that has settled into the shape of a Smartie. They can just cope with life on the edge, where the gravity is only about 3 G, but can't go anywhere near the poles. However, they encounter a wandering trader, a caterpillar-like creature navigating a raft.

It also set me wondering about a similar problem. You are a maintenance man on the space station in the film 2001, which is a large torus

revolving at a speed to create 1 G on the floor at the outer edge of the ring—but not so large as to have any noticeable gravitational effect of its own. You have to go outside to mend something on the outer edge of the hull. Your lifeline becomes unhooked, so I suppose you now proceed at a steady speed in a straight line tangential to the outer edge of the ring.

However, G is defined as an acceleration of 9.81 metres per second per second. As seen from the centre of the ring, at what velocity are you departing?

Best wishes,

Ralph Hancock

Hotels

Dear Tony,

Re: Solution 202.3 – The puzzled hotelier. [See M500 225, page 16. The original problem in M500 **202** was to determine the (unique) set of consecutive room numbers in the range 101–199 using information gleaned from this conversation between me and an hotelier.

"They were," he said, "off four corridors forming a square and ordered so that the sums of pairs of numbers of adjacent rooms were all primes."

He told me how many rooms there were, and I countered, "There couldn't have been fewer."]

Did Steve Moon decide that the number of rooms must be a multiple of four because there are four sides to a square? The respective numbers of rooms on each of the four corridors aren't necessarily the same.

The sequence of primes, not less than $101 + 102 = 203$ starts 211, 223, ... and since $223 - 101$ is 122 there must be at least 22 rooms. This is the solution if and only if there is some cycle of that order consistent with the data. And there is. Probably more than one cycle because of the higher potential degrees of some of the vertices, for example vertices (the rooms) 119 and 120 have potential degree equal to 6. One possibility:

101, 110, 113, 116, 107, 104, 119, 114, 109, 102, 121,
120, 103, 108, 115, 112, 111, 118, 105, 106, 117, 122, (101).

Ian Adamson

Steve Moon showed that the solution to this problem was 24 rooms and listed one possible sequence of rooms. He wondered how many other sequences of room numbers satisfied the given conditions.

If we ignore the position of the start room number 101 and whether we go round the corridor clockwise or anti-clockwise then the number of solutions is 22,842.

I have also looked at the solutions of the problem for all start room numbers up to 500. It is clear that the only possible set of room numbers for a hotel with 4 rooms is 2-1-4-3-. The lowest starting room numbers which require 8, 12, 16, 20, 24, 28 and 32 rooms are 2, 4, 35, 52, 94, 230, and 254 respectively.

If we also impose the restriction that there is a unique solution then the corresponding starting room numbers are 6, 19, 36, 118, 156, 250, 381, and unknown. These are shown below.

9-8-11-12-7-6-13-10-

22-25-28-19-24-29-30-23-20-27-26-21-

119-122-129-128-123-118-133-124-127-130-121-120-131-126-125-132-

159-158-173-164-167-170-161-156-175-162-169-168-163-174-157-160-171-166-165-172-

261-260-263-258-265-256-267-254-269-272-251-252-271-270-253-250-273-268-255-266-257-264-259-262-

394-393-404-383-386-387-400-397-390-407-402-395-392-381-406-405-382-391-396-401-408-389-398-399-388-385-384-403-

Dave Wild

Problem 228.2 – Arithmetic progression

Martin Hansen

An arithmetic progression contains only positive integer terms. The sum of the first three terms is 51. The sum of the last four terms is 332. Show that only two arithmetic progressions satisfy these conditions and list those two progressions.

Problem 228.3 – Another arithmetic progression

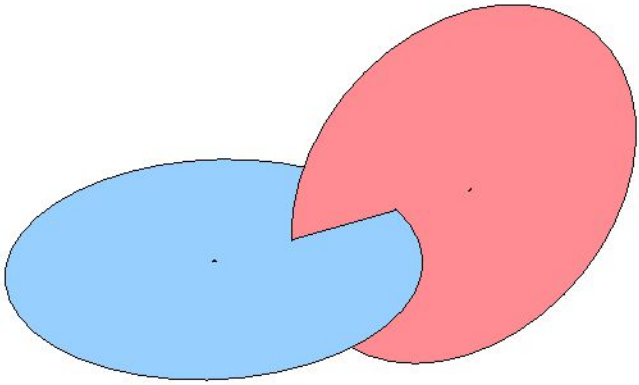
The three sides of a triangle are in arithmetic progression with common difference 1. The largest angle exceeds the smallest by 90°.

What are the sides?

Mathematics in the kitchen – VI
Tony Forbes

Following the trend we started in M500 **188** and continued occasionally since then (the last one being M500 **225**), here is yet another experiment that you can perform with materials available in any well-equipped kitchen.

You will need two matching circular table mats or similar, such beer mats, or flattened paper plates, or in fact any pair of identical discs. Ideally they should be very thin but rigid. You will also need a knife and some glue. Make a slot in one of the discs along a radius and measuring exactly $2 - \sqrt{2} \approx 0.5858$ radius-lengths. The thickness of the slot should be the same as that of the material. Insert the other disc into the slot so that the two discs are orthogonal to each other. Glue the assembly together. You should end up with the two discs joined at right-angles to each other with their centres $\sqrt{2}$ radius-lengths apart.



Now let the thing roll around on a perfectly flat kitchen worktop. If your workmanship was sufficiently accurate, you will observe that there is no unique stable position. The object naturally moves around just like a perfect cylinder. In other words, the centre of gravity is always at the same height above the surface.

Can you explain why? Is the ratio $\sqrt{2}$ special?

Thanks to **Dick Boardman** for the idea behind this experiment.

Warning. Solvent-based gluing substances should always be used with care and in a well-ventilated environment. *Do not perform the experiment if you are unwilling to take responsibility for accidents.*

Numbers on the brain

Rob Evans

This article shall be concerned with Problem 152.2. For those readers who do not have a copy of M500 **152** to hand, a verbatim wording of that problem follows.

> Algernon and Charles are seated, facing each other. Each has a piece of card attached to his forehead on which is written a positive integer. Each can see the other's number, but not his own. On a blackboard which both can see are written two positive integers. They know that one of these numbers is the sum of the numbers on their foreheads, but they do not know which one it is. They take it in turns to ask each other: "Do you know the number on your forehead?" Will it always be the case that one or other of them will eventually be able to answer "Yes" to this question?

Unfortunately, the above wording is not a very clear statement of the problem that I think that the author(s) had in mind. I think that they intended that there should be no transfer of information between Algernon and Charles by way of hand signals; variations in the way they speak; variations in the length of the intervening periods of silence etc. If I am right about this then I am almost certain that the answer to the question posed at the end of the problem has to be "No". However, if I am wrong about this then I am absolutely certain that (assuming the existence of a suitable agreement beforehand between Algernon and Charles on how to interpret each other's actions) the answer to that question is "Yes". One possible course of action for them to take would be to agree beforehand on a suitable 'unit of time' (e.g. one second) and then proceed as follows.

(1) Algernon to ask: "Do you know the number on your forehead?"

(2) Charles to remain silent for a period of time whose length (as measured in terms of the agreed unit of time) is equal to the number on Algernon's forehead.

(3) Charles to ask: "Do you know the number on your forehead?"

(4) Algernon to answer "Yes" to the question asked in (3).

(N.B. Algernon's answer is *truthful* since he knows that the number on his forehead is equal to the length (as measured in terms of the agreed unit of time) of the period of silence in (2).)

This course of action has the advantage that knowledge of the number on Algernon's forehead is transferred by Charles to Algernon in a particularly inconspicuous way (à la Derren Brown, perhaps?). But, as I indicated before, this is just one possible course of action. There are (as readers can confirm) many others.

So, depending on which interpretation one has of the author's(s') original wording, the answer to the question posed at the end of the problem seems to be either an obvious "No" or an obvious "Yes". Either way the problem does not seem to be very interesting. All this leaves me thinking that I might have got hold of the wrong end of the stick! In which case, if any reader can provide clarification of the problem then I would be most grateful if they did so.

Problem 228.4 – Perfection

Tony Forbes

This is based on Number 128 of Robin Whitty's *Theorem of the day*,

http://www.theoremoftheday.org/Theorems.html.

A *perfect number*, is a positive integer, N, for which the sum of the divisors of N is $2N$; in symbols, $\sum_{d|N} d = 2N$. The sequence begins

6, 28, 496, 8128, 33550336, 8589869056, 137438691328,
2305843008139952128, 2658455991569831744654692615953842176,
191561942608236107294793378084303638130997321548169216, ...

Prove the following assertions.

(i) The number N is perfect iff $\sum_{d|N} 1/d = 2$.

(ii) An even number N is perfect iff $N = 2^{p-1}(2^p - 1)$ for some prime $2^p - 1$.

(iii) All even perfect numbers end in 6 or 28.

(iv) An even perfect number has digital root 1. To compute the digital root of a positive integer n, replace n by the sum of its decimal digits, and then repeat this process at least $\log n$ times.

(v) A sufficiently large even perfect number is the sum of the first few odd cubes.

And if you have time,

(vi) decide whether the qualifier 'even' can be removed from items (ii)–(v), above.

Right-angled triangles

Chris Pile

Using generators p, q to give $x = p^2 - q^2$, $y = 2pq$, $z = p^2 + q^2$, we can create triangles in pairs with either $x + y$ square or z square [see Problem 225.2 – Pythagorean triangles].

$x+y$ is a square				z is a square				
p	q	$x+y$	$p-q$	p	q	z	$p+q$	$p-q$
5	4	$49 = 7^2$	1	4	3	$25 = 5^2$	7	1
13	6	$289 = 17^2$	7	12	5	$169 = 13^2$	17	7
25	8	$961 = 31^2$	17	24	7	$625 = 25^2$	31	17
17	10	$529 = 23^2$	7	15	8	$289 = 17^2$	23	7
41	10	$2401 = 49^2$	31	40	9	$1681 = 41^2$	49	31
61	12	$5041 = 71^2$	49	60	11	$3721 = 61^2$	71	49
37	14	$2209 = 47^2$	23	35	12	$1369 = 37^2$	47	23
85	14	$9409 = 97^2$	71	84	13	$7225 = 85^2$	97	71
113	16	$16129 = 127^2$	97	112	15	$12769 = 113^2$	127	97
65	18	$6241 = 79^2$	47	63	16	$4225 = 65^2$	79	47
145	18	$25921 = 161^2$	127	144	17	$21025 = 145^2$	161	127
181	20	$39601 = 199^2$	161	180	19	$32761 = 181^2$	199	161
101	22	$14161 = 119^2$	79	99	20	$10201 = 101^2$	119	79
221	22	$58081 = 241^2$	199	220	21	$48841 = 221^2$	241	199

Note that the two $p - q$ columns are the same. Also $z \pm y$ is a square, but $x + z$ is never a square. The generator p in the $(x + y)$-square triangle becomes $p^2 = z$ in the z-square triangle. The $p+q$ column for the z triangle becomes $(p + q)^2 = x + y$ in the $(x + y)$ triangle.

The nearest to having $x + y$ and z both square for small integers is $(161, 240, 289)$, with $x + y = 401 = 20^2 + 1$ and $z = 17^2$.

Composite triangles can be formed, such as

$$(15129, 67240, 68921), \qquad x + y = 82369 = 287^2, \qquad z = 41^3.$$

Several triangles were revealed having the same hypotenuse. Here are some examples with $z = 4225 = 65^2$.

1040, 4095, 4225	2535, 3380, 4225
1183, 4056, 4225	2975, 3000, 4225
1625, 3900, 4225	3289, 2652, 4225
2047, 3696, 4225	3713, 2016, 4225

Problem 228.5 – Square roots

Dick Boardman

Given that

$$(\sqrt{a} - \sqrt{a-1})^n \;=\; \sqrt{b} - \sqrt{b-1},$$

Show that for any positive integer n, b is an integer if a is an integer.

M500 Mathematics Revision Weekend 2009

The thirty-fifth **M500 Society Mathematics Revision Weekend** will be held at

Aston University, **Birmingham**

over

Friday $11^{\mathbf{th}}$ – **Sunday** $13^{\mathbf{th}}$ **September 2009**.

The cost, including accommodation (with en suite facilities) and all meals from bed and breakfast Friday night to lunch Sunday is £234 (in Aston's Lakeside flats) or £278 (Aston Business School), The cost for non-residents is £115 (includes Saturday and Sunday lunch). M500 members get a discount of £10. For full details and an application form, see the Society's web site at www.m500.org.uk, or send a stamped, addressed envelope to

Jeremy Humphries, M500 Weekend 2009.

The Weekend is open to all Open University students, and is designed to help with revision and exam preparation. We expect to present the following mathematics-based OU courses, subject to sufficient numbers:

> M208, M248, M256, M337, M343, M346, M359, M362, M363, M366, M373, M381, M820, M821, M823, MS221, MST209, MST326 and MT365.

Tutorial sessions start at 19.30 on the Friday and finish at 17.00 on the Sunday.

As usual, on the Saturday evening we have a break from tutorials. Rob Rolfe will be running a pub quiz with Valuable Prizes, and we plan to organize a guest lecture on a popular mathematical topic—consult the web site for details nearer the time.

The last date for receipt of bookings is 20th August 2009.

Contents M500 228 – June 2009

Cover: The Gewirtz graph. The vertices are the 56 blocks of the Steiner system $S_4(2, 6, 21)$, and two vertices are joined when the blocks they represent are disjoint [http://mathworld.wolfram.com/GewirtzGraph.html].