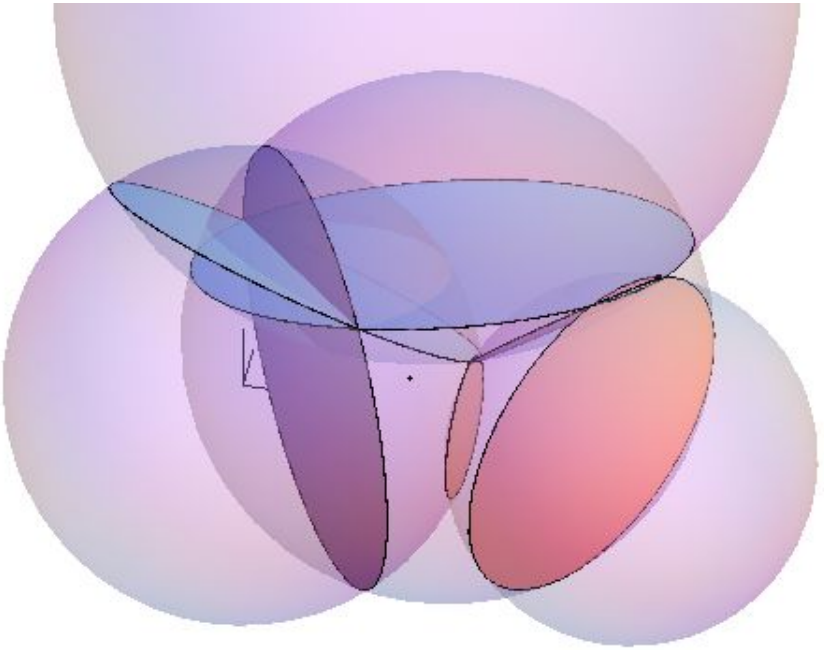
*

ISSN 1350-8539

M500

M500 261



The M500 Society and Officers

The M500 Society is a mathematical society for students, staff and friends of the Open University. By publishing M500 and by organizing residential weekends, the Society aims to promote a better understanding of mathematics, its applications and its teaching. Web address: m500.org.uk.

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

The Revision Weekend is a residential Friday to Sunday event providing revision and examination preparation for both undergraduate and postgraduate students. For 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.

Solution 259.4 – Double integrals

(i) Suppose $a^2 + b^2 = 1$. Show that

$$I \;=\; \int_0^{\pi/2}\int_0^{\pi/2} \frac{a^2\cos^2\theta + b^2\cos^2\phi}{\sqrt{1-a^2\sin^2\theta}\sqrt{1-b^2\sin^2\phi}}\,d\theta\,d\phi \;=\; \frac{\pi}{2}.$$

(ii) Suppose $a, b, c > 0$. Show that

$$J \;=\; \int_0^{a}\int_0^{b} \frac{c\,dx\,dy}{(c^2+x^2+y^2)^{3/2}} \;=\; \arctan\frac{ab}{c\sqrt{a^2+b^2+c^2}}.$$

Steve Moon

First part

As it stands this looks relatively intractable. But we can transform the numerator,

$$a^2\cos^2\theta + b^2\cos^2\phi \;=\; (1-a^2\sin^2\theta) + (1-b^2\sin^2\phi) - 1$$

(using $a^2 + b^2 = 1$), and then write I thus:

$$\begin{aligned} I \;=\; &\int_0^{\pi/2}\int_0^{\pi/2} \frac{\sqrt{1-a^2\sin^2\theta}}{\sqrt{1-b^2\sin^2\phi}}\,d\theta\,d\phi + \int_0^{\pi/2}\int_0^{\pi/2} \frac{\sqrt{1-b^2\sin^2\phi}}{\sqrt{1-a^2\sin^2\theta}}\,d\theta\,d\phi \\ &- \int_0^{\pi/2}\int_0^{\pi/2} \frac{1}{\sqrt{1-a^2\sin^2\theta}\sqrt{1-b^2\sin^2\phi}}\,d\theta\,d\phi, \end{aligned}$$

where each of these integrals is separable into elliptic integrals.

In standard notation the *complete elliptic integral of the first kind* is

$$K(a) \;=\; \int_0^{\pi/2} \frac{d\theta}{\sqrt{1-a^2\sin^2\theta}},$$

where $0 \le a \le 1$ and we denote this integral as complete because the upper limit is at the maximum permissible range in $[0, \pi/2]$. Similarly we have the *complete elliptic integral of the second kind*,

$$E(a) \;=\; \int_0^{\pi/2} \sqrt{1-a^2\sin^2\theta}\,d\theta.$$

Hence we can express I in terms of complete elliptic integrals,

$$\begin{aligned} I \;&=\; E(a)K(b) + E(b)K(a) - K(a)K(b) \\ &=\; E(a)K(\sqrt{1-a^2}) + E(\sqrt{1-a^2})K(a) - K(a)K(\sqrt{1-a^2}). \end{aligned} \qquad (1)$$

If we did not know the form of the answer, we might suspect a dependence upon a. We can investigate this by treating a as an independent variable and considering $dI(a)/da$. We need $dE(a)/da$, $dE(b)/da$, $dK(a)/da$, $dK(b)/da$ and proceed by differentiating under the integral sign. Thus

$$\frac{dE(a)}{da} \;=\; \frac{d}{da}\int_0^{\pi/2} \sqrt{1-a^2\sin^2\theta}\,d\theta \;=\; \int_0^{\pi/2} \frac{-a\sin^2\theta}{\sqrt{1-a^2\sin^2\theta}}\,d\theta.$$

Therefore

$$a\frac{dE(a)}{da} \;=\; \int_0^{\pi/2}\left(\frac{1-a^2\sin^2\theta}{\sqrt{1-a^2\sin^2\theta}} - \frac{1}{\sqrt{1-a^2\sin^2\theta}}\right)d\theta \;=\; E(a)-K(a);$$

hence

$$\frac{dE(a)}{da} \;=\; \frac{E(a)-K(a)}{a} \tag{2}$$

and

$$\frac{dE(b)}{da} \;=\; \frac{dE(b)}{db}\frac{db}{da} \;=\; -\frac{a}{b^2}\big(E(b)-K(b)\big) \tag{3}$$

since $db/da = -a/b$. Also

$$\begin{aligned}\frac{dK(a)}{da} \;&=\; \frac{d}{da}\int_0^{\pi/2}\frac{d\theta}{\sqrt{1-a^2\sin^2\theta}} \;=\; \int_0^{\pi/2}\frac{a\sin^2\theta}{(1-a^2\sin^2\theta)^{3/2}}\,d\theta \\ &=\; \frac{1}{a}\left(\int_0^{\pi/2}\frac{d\theta}{(1-a^2\sin^2\theta)^{3/2}} - K(a)\right).\end{aligned} \tag{4}$$

The remaining integral looks awkward, and I needed a pointer from the Internet to get the identity

$$\begin{aligned}&\frac{\sqrt{1-a^2\sin^2\theta}}{1-a^2} - \frac{a^2}{1-a^2}\cdot\frac{d}{d\theta}\left(\frac{\sin\theta\cos\theta}{\sqrt{1-a^2\sin^2\theta}}\right) \\ &=\; \frac{\sqrt{1-a^2\sin^2\theta}}{1-a^2} - \frac{a^2}{1-a^2}\left(\frac{\cos^2\theta-\sin^2\theta}{\sqrt{1-a^2\sin^2\theta}}\right) - \frac{a^4}{1-a^2}\,\frac{\cos^2\theta\sin^2\theta}{(1-a^2\sin^2\theta)^{3/2}} \\ &=\; \frac{(1-a^2\sin^2\theta)^2 - a^2(\cos^2\theta-\sin^2\theta)(1-a^2\sin^2\theta) - a^4\sin^2\theta\cos^2\theta}{(1-a^2)(1-a^2\sin^2\theta)^{3/2}} \\ &=\; \frac{1}{(1-a^2\sin^2\theta)^{3/2}}.\end{aligned}$$

Therefore

$$\int_0^{\pi/2} \frac{d\theta}{(1-a^2\sin^2\theta)^{3/2}} \;=\; \frac{E(a)}{1-a^2} - \frac{a^2}{1-a^2}\left[\frac{\sin\theta\cos\theta}{\sqrt{1-a^2\sin^2\theta}}\right]_0^{\pi/2} \;=\; \frac{E(a)}{1-a^2},$$

and hence from (4),

$$\frac{dK(a)}{da} \;=\; \frac{E(a)}{a(1-a^2)} - \frac{K(a)}{a}. \tag{5}$$

Finally, recalling that $b^2 = 1-a^2$ and hence $db/da = -a/b$,

$$\frac{dK(b)}{da} \;=\; \left(\frac{E(b)}{b(1-b^2)} - \frac{K(b)}{b}\right)\cdot\frac{-a}{b} \;=\; -\frac{E(b)}{ab^2} + \frac{aK(b)}{b^2}. \tag{6}$$

From differentiating (1) with respect to a,

$$\begin{aligned}\frac{dI}{da} \;=\;& K(b)\frac{dE(a)}{da} + E(a)\frac{dK(b)}{da} + K(a)\frac{dE(b)}{da} + E(b)\frac{dK(a)}{da} \\ & - K(b)\frac{dK(a)}{da} - K(a)\frac{dK(b)}{da}.\end{aligned}$$

Substituting for the various derivatives using (2), (3), (5) and (6), after some straightforward manipulation using $a^2+b^2=1$ the right hand side eventually simplifies to zero. Hence we have shown that that I is equal to some constant independent of a.

In general elliptic integrals are not readily evaluated analytically; but we can choose any value of a, say $a = 0$ or 1. Now from the definitions,

$$E(0) \;=\; K(0) \;=\; \int_0^{\pi/2} d\theta \;=\; \frac{\pi}{2}$$

and

$$E(1) \;=\; \int_0^{\pi/2} \sqrt{1-\sin^2\theta}\,d\theta \;=\; \int_0^{\pi/2} (\cos\theta)\,d\theta \;=\; 1.$$

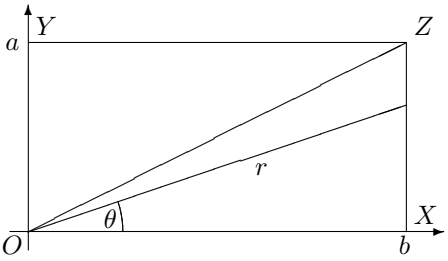
Hence, putting $a = 0$ in (1), we have

$$I \;=\; E(0)K(1) + E(1)K(0) - K(0)K(1) \;=\; \frac{\pi}{2},$$

as required.

Second part

The integration in J is over a rectangular domain but the presence of $x^2 + y^2$ indicates polar coordinates might be useful.



We divide the domain into two parts, triangles OXZ and OYZ. Then with $x^2 + y^2 = r^2$ and $dx\,dy = r\,dr\,d\theta$ we have over OXZ

$$\begin{aligned} J_1 &= \int_0^{\arctan\frac{a}{b}} \int_0^{b\sec\theta} \frac{cr}{(c^2+r^2)^{3/2}}\,dr\,d\theta \\ &= \int_0^{\arctan\frac{a}{b}} \left(1 - \frac{c}{\sqrt{c^2+b^2\sec^2\theta}}\right) d\theta \end{aligned} \tag{1}$$

and over OYZ

$$\begin{aligned} J_2 &= \int_{\arctan\frac{a}{b}}^{\pi/2} \int_0^{a\,\mathrm{cosec}\,\theta} \frac{cr}{(c^2+r^2)^{3/2}}\,dr\,d\theta \\ &= \int_{\arctan\frac{a}{b}}^{\pi/2} \left(1 - \frac{c}{\sqrt{c^2+b^2\,\mathrm{cosec}^2\,\theta}}\right) d\theta. \end{aligned} \tag{2}$$

Therefore, combining (1) and (2), the integral in the problem becomes

$$\begin{aligned} J &= J_1 + J_2 \\ &= \frac{\pi}{2} - \int_0^{\arctan\frac{a}{b}} \frac{c\,d\theta}{\sqrt{c^2+b^2\sec^2\theta}} - \int_{\arctan\frac{a}{b}}^{\pi/2} \frac{c\,d\theta}{\sqrt{c^2+b^2\,\mathrm{cosec}^2\,\theta}} \\ &= \frac{\pi}{2} - \int_0^{\arctan\frac{a}{b}} \frac{c(\cos\theta)\,d\theta}{\sqrt{b^2+c^2\cos^2\theta}} - \int_{\arctan\frac{a}{b}}^{\pi/2} \frac{c(\sin\theta)\,d\theta}{\sqrt{a^2+c^2\sin^2\theta}}. \end{aligned} \tag{3}$$

Now we would like to get the second integral in (3) into a similar form to the first. If we set $\theta = \pi/2 - \phi$, then $\sin\theta = \cos\phi$, $d\theta = -d\phi$, and $\theta = \arctan a/b \Rightarrow \phi = \arctan b/a$. Therefore

$$\int_{\arctan\frac{a}{b}}^{\pi/2} \frac{c(\sin\theta)\,d\theta}{\sqrt{a^2+c^2\sin^2\theta}} = \int_{\arctan\frac{b}{a}}^{0} \frac{c(\cos\phi)\,d\phi}{\sqrt{a^2+c^2\cos^2\phi}} \tag{4}$$

and resuming from (3) after simply replacing ϕ by θ in (4) for tidiness as

well as flipping the sign and reversing the limits,

$$\begin{aligned} J &= \frac{\pi}{2} - \int_0^{\arctan\frac{a}{b}} \frac{c(\cos\theta)\,d\theta}{\sqrt{b^2+c^2\cos^2\theta}} - \int_0^{\arctan\frac{b}{a}} \frac{c(\cos\theta)\,d\theta}{\sqrt{a^2+c^2\cos^2\theta}} \\ &= \frac{\pi}{2} - \int_0^{\arctan\frac{a}{b}} \frac{c(\cos\theta)\,d\theta}{\sqrt{b^2+c^2-c^2\sin^2\theta}} - \int_0^{\arctan\frac{b}{a}} \frac{c(\cos\theta)\,d\theta}{\sqrt{a^2+c^2-c^2\sin^2\theta}}. \end{aligned}$$

Substituting $u = c\sin\theta$, $du = c\cos\theta$ and noting that $\theta = \arctan x/y$ implies $u = c\sin\theta = xc/\sqrt{x^2+y^2}$, we have

$$\begin{aligned} J &= \frac{\pi}{2} - \int_0^{\frac{ac}{\sqrt{a^2+b^2}}} \frac{du}{\sqrt{b^2+c^2-u^2}} - \int_0^{\frac{bc}{\sqrt{a^2+b^2}}} \frac{du}{\sqrt{a^2+c^2-u^2}} \\ &= \frac{\pi}{2} - \left[\arcsin\left(\frac{u}{\sqrt{b^2+c^2}}\right)\right]_0^{\frac{ac}{\sqrt{a^2+b^2}}} - \left[\arcsin\left(\frac{u}{\sqrt{a^2+c^2}}\right)\right]_0^{\frac{bc}{\sqrt{a^2+b^2}}} \\ &= \frac{\pi}{2} - \arcsin\left(\frac{ac}{\sqrt{a^2+b^2}\sqrt{b^2+c^2}}\right) - \arcsin\left(\frac{bc}{\sqrt{a^2+b^2}\sqrt{a^2+c^2}}\right) \\ &= \arccos\left(\frac{ac}{\sqrt{a^2+b^2}\sqrt{b^2+c^2}}\right) - \arcsin\left(\frac{bc}{\sqrt{a^2+b^2}\sqrt{a^2+c^2}}\right). \end{aligned}$$

Now we can think of these two expressions as angles θ_1 and θ_2 respectively. Then

$$\tan J = \tan(\theta_1 - \theta_2) = \frac{\tan\theta_1 - \tan\theta_2}{1 + (\tan\theta_1)(\tan\theta_2)}. \tag{5}$$

Moreover,

$$\begin{aligned} \tan\theta_1 &= \frac{\sqrt{(a^2+b^2)(b^2+c^2)-a^2c^2}}{ac} = \frac{b\sqrt{a^2+b^2+c^2}}{ac}, \\ \tan\theta_2 &= \frac{bc}{\sqrt{(a^2+b^2)(a^2+c^2)-b^2c^2}} = \frac{bc}{a\sqrt{a^2+b^2+c^2}}. \end{aligned}$$

Substitute these expressions into (5) and simplify:

$$\tan J = \frac{\dfrac{b\sqrt{a^2+b^2+c^2}}{ac} - \dfrac{bc}{a\sqrt{a^2+b^2+c^2}}}{1+\dfrac{b^2}{a^2}} = \frac{ab}{c\sqrt{a^2+b^2+c^2}}.$$

Hence

$$J = \arctan\frac{ab}{c\sqrt{a^2+b^2+c^2}}.$$

Solution 259.1 – Four primes

Find a number n such that n is the product of four distinct primes and every group of order n is Abelian.

Stuart Walmsley

Introduction

The key result needed to solve this problem is established. It is found that there are many numbers which have the property specified. An alternative version is suggested: to find n such that the number of non-Abelian groups takes the maximum possible value. Examples are given of numbers which satisfy both criteria.

The problem is concerned with numbers n which are the product of four distinct primes, that is $n = pqrs$ in which it is assumed that $p > q > r > s$.

Groups with prime number order

Start with one prime number p. A group of order p must contain an element of order p. This element generates a cycle of order p, giving a cyclic (Abelian) group of order p, denoted C_p. Hence there is only one group of order p and it is Abelian. One element of the group, the identity I, has order 1. The other $p - 1$ elements are of order p and any one of them may be used to generate the group.

Abelian groups of order $pqrs$

Every finite Abelian group may be expressed as a direct product of cyclic groups, the order of each of which is a power of a prime number. For the number n under consideration, there is only one possible arrangement

$$C_p \times C_q \times C_r \times C_s \;=\; C_{pqrs};$$

that is, a cyclic group of order n, since p, q, r, s are coprime. There is only one Abelian group of order $pqrs$.

Groups of order pq

The possible occurrence of a non-Abelian group is most easily explained by directing attention to the simpler case of pq $(p > q)$. There can be no element of order pq since this would generate the Abelian group C_{pq}.

Specifically, consider $n = 6 = 3 \cdot 2$. Let A be a group element of order 3 and B of order 2. Then

$$A^3 \;=\; I, \quad B^2 \;=\; I,$$

where I is the identity. Then the six elements of the group may be written

$$I, \quad A, \quad A^2, \quad B, \quad AB, \quad A^2B.$$

But BA must be one of the group elements, other than a power of A or B. There are therefore two possibilities:

$$BA = AB, \quad \text{or} \quad BA = A^2B.$$

In the first case, the group is Abelian and AB is of order 6 with successive powers

$$AB, \quad A^2, \quad B, \quad A, \quad A^2B, \quad I$$

and the group has the structure $C_3 \times C_2 \equiv C_6$. In the second case, the group is non-Abelian and the elements B, AB, A^2B are all of order 2. It is the well known dihedral group of order 6.

This result may be generalized in the following way. The group order is pq and A an element of p and B of order q ($< p$). A non-Abelian group exists if there is a consistent relationship of the form $BA = A^jB$. Then successively

$$BA = A^jB, \quad B^2A = A^{2j}B^2, \quad \ldots;$$

but $B^q = I$, so that A and B^q commute,

$$B^qA = A^{qj}B^q = AB^q \quad \text{and} \quad A^{qj} = A.$$

Successive powers of B take A through a cycle of non-zero powers of A: a cycle of length q which ends at A. All non-zero powers of A must behave in the same way, so that they are divided into subsets of length q. Hence q must be a factor of $p - 1$.

This is the key result: q must be a factor of $p - 1$.

For an odd prime p, $p - 1$ is even and $q = 2$ always fulfils the required condition for a non-Abelian group. This gives rise to the familiar (non-Abelian) dihedral group of order $2p$.

$$A^p = I, \quad B^2 = I, \quad BA = A^{p-1}B.$$

When $q = 3$, q is a factor of $p - 1$ for about half the higher primes, for example $p = 7$. In this case, the group may be defined by

$$A^7 = I, \quad B^3 = I, \quad BA = A^2B$$

and

$$BA = A^2B, \quad B^2A = A^4B^2, \quad B^3A = A^8B^3 = AB^3.$$

Furthermore, using the defining relations,

$$BA^7 = A^6B, \quad B^2A^7 = A^3B^2, \quad B^3A^7 = A^7B^3$$

so that the six non-zero powers of A are split into two sets of three under the influence of B.

The factor A^2 in the third defining relationship has to be found by trial and error, although theory establishes that the relationship exists. This is in fact the smallest non-Abelian group of odd order.

For higher values of q, the condition for finding a non-Abelian group is satisfied less and less frequently. For example, there are Abelian groups for the following pairs pq.

$q = 3$	$p = 7, 13, 19, 31, 37, 43, \ldots$	$q = 5$	$p = 11, 31, 41, 61, \ldots$
$q = 7$	$p = 29, 43, 71, \ldots$	$q = 11$	$p = 23, 67, 89, \ldots$
$q = 13$	$p = 53, 79, 131, \ldots$	$q = 17$	$p = 103, 137, 229, \ldots$

This can be expressed by saying that a non-Abelian group can be constructed when $2fq + 1$ is a prime p (f a positive integer).

Groups of order $pqrs$

When the group is extended to the case under consideration, $n = pqrs$, the condition for no non-Abelian group takes the same basic form repeated many times. Thus any of the prime numbers must not be a factor of any higher prime minus one. For a group of order $pqrs$, with $p > q > r > s$ to have no non-Abelian groups:

s must NOT be a factor of $r - 1$ OR of $q - 1$ OR of $p - 1$

AND r must NOT be a factor of $q - 1$ OR of $p - 1$

AND q must NOT be a factor of $p - 1$.

It is then possible to construct examples avoiding the pairs of primes above which do give non-Abelian groups. In this way $3 \cdot 5 \cdot 17 \cdot 23$ fits the conditions. As a check the factors of p and $p - 1$ etc. are given.

$3 = 3$	$5 = 5$	$17 = 17$	$23 = 23$
$2 = 2$	$4 = 2 \cdot 2$	$16 = 2 \cdot 2 \cdot 2 \cdot 2$	$22 = 2 \cdot 11$

In fact, the number of examples is legion particularly if 3 and 5 are avoided. For example, four closely spaced primes frequently satisfy the conditions.

One possibility is $7 \cdot 11 \cdot 13 \cdot 17$, and another, $11 \cdot 13 \cdot 17 \cdot 19$. Indeed any four of these five, would provide further examples. As a check the factors of p and $p-1$ etc are given.

$7 = 7$	$11 = 11$	$13 = 13$	$17 = 17$	$19 = 19$
$6 = 2 \cdot 3$	$10 = 2 \cdot 5$	$12 = 2 \cdot 2 \cdot 3$	$16 = 2 \cdot 2 \cdot 2 \cdot 2$	$18 = 2 \cdot 3 \cdot 3$

Find n such that n is the product of four distinct primes and the maximum possible number of groups of order n is non-Abelian

Numbers n with the maximum number of non-Abelian groups are much rarer. The conditions are reversed. For the maximum number of non-Abelian groups, each term must be a factor of all higher terms minus one. Thus:

s IS a factor of $r-1$, AND of $q-1$ AND of $p-1$

AND r IS a factor of $q-1$ AND of $p-1$

AND q IS a factor of $p-1$.

Examination of the table of allowed pairs show that a suitable value is $2 \cdot 3 \cdot 7 \cdot 43$. The value 2 always leads to non-Abelian groups for all higher primes. An example of an odd number with the required property is $3 \cdot 7 \cdot 43 \cdot 3613$. Check prime factors of p and $p-1$ etc.

$3 = 3$	$7 = 7$	$43 = 43$	$3613 = 3613$
$2 = 2$	$6 = 2 \cdot 3$	$42 = 2 \cdot 3 \cdot 7$	$3612 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 43$

Examples can be constructed by taking a prime s and then finding a prime of the form $r = 2ds + 1$, followed by a prime of the form $q = 2ers + 1$ and then a prime of the form $p = 2fqrs + 1$, where d, e and f are integers. In the above example $d = 1$, $e = 1$ and $f = 2$.

Problem 261.1 – Polynomial factorization

As is well known, the polynomial $x^4 + 1$ is irreducible over the integers. However there exist various factorizations if the domain is extended slightly,

$$\begin{aligned} x^4 + 1 &= (x^2 + i)(x^2 - i) \\ &= (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \\ &= (x^2 + \sqrt{2}\,ix - 1)(x^2 - \sqrt{2}\,ix - 1), \end{aligned}$$

or if we work modulo something. Show that for any prime p, there exists a non-trivial factorization of $x^4 + 1$ modulo p. For instance, $x^4 + 1 \equiv (x^2 + 4)(x^2 - 4) \pmod{17}$.

Short exact sequences and group extensions

Tommy Moorhouse

Introduction

Short exact sequences may sound mysterious but they crop up in many applications and are actually quite simple to get to grips with. Here, after a brief introduction, we'll use them in a construction known as a group extension, and we'll find two different extensions of $\mathbb{Z}_3$.

Definitions

A sequence of maps between spaces

$$0 \to G \xrightarrow{\alpha} H \xrightarrow{\beta} W \to 0$$

is called a short exact sequence if at each stage the image of the left map is the kernel of the right map. To gain an understanding of what this means, let's look at the first map at G, which we will call $i : \{0\} \to G$. The image of this map must be the identity element e_G of G since α is a group homomorphism. We call the map from G to H α. The image of i is then the kernel of α. This means that $\alpha(e_G) = e_H$, where we have temporarily used a subscript on e to indicate which group it belongs to. This in turn means that α must be one-to-one (injective) since the cosets of e relative to e_G are just the elements of G, and each such coset maps to a different element of H under α.

We call the map from H to W β. At H the image of α is the kernel of β: $\beta \circ \alpha(g) = 0$ for all $g \in G$.

Finally we examine the sequence at W. The whole of W is mapped to a single element. This means that the whole of W is the image of H under β and so β is onto (surjective).

A short exact sequence thus defines a very definite structure. The maps are restricted and, effectively, we have $G \sim H/W$, with appropriate interpretations of G and W.

Group extensions – two examples The idea of a short exact sequence can be used to enlarge a given group by 'multiplying' it by another group. The examples we will consider are both extensions of $\mathbb{Z}_3$ by $\mathbb{Z}_2$, but they are not isomorphic. In fact one is abelian and the other is not.

A short exact sequence of groups such as the one above is said to exhibit H as an extension of G by W. A little examination shows that the order of H in our case is 6. We write the elements of $\mathbb{Z}_3$ as the integers $0, 1, 2$

with the group operation being addition modulo 3. Notice that this group is isomorphic to the group of rotational symmetries of the equilateral triangle.

The first case we consider is when H is the cyclic group of order 6 consisting of the integers $\{0, 1, 2, 3, 4, 5\}$ under addition modulo 6. This group is isomorphic to the rotational symmetry group of the regular hexagon. The map α defined by

$$\alpha(0) \;=\; 0, \quad \alpha(1) \;=\; 2, \quad \alpha(2) \;=\; 4$$

sends $\mathbb{Z}_3$ to the subgroup of H of order 3. Then β sends the elements of H to their parity (i.e. odd integers are mapped to 1 while even integers are mapped to 0). This gives the desired short exact sequence, as you can check.

The nonabelian case is similar. Here we write H multiplicatively, as is usual for nonabelian groups; H consists of the elements $1, a, a^2, c, ac$ and ca, a notation chosen for convenience (we could have written ac as d and ca as g for example). The group table can be constructed from the rule that

$$c^2 \;=\; 1, \quad a^3 \;=\; 1, \quad (ac)^2 \;=\; (ca)^2 \;=\; 1 \;\text{ and }\; ac \;\neq\; ca.$$

This group is isomorphic to the full group of symmetries of the plane equilateral triangle, including reflections. We choose α to be the map sending 0 to 1, 1 to a and 2 to a^2. Then the choice of β onto $\mathbb{Z}_2$ is fairly obvious, and you just need to check that it a group homomorphism.

Summary This construction allows the formulation of nonabelian groups from abelian ones. It is interesting to explore other examples of low order to get a feel for what it is all about. As we have noted, the groups involved have a natural interpretation acting on geometrical objects and this can also help to visualise the maps and what they tell us about the extended group.

Useful Books [Lang] is a thorough, if sometimes challenging, book on the fundamental ideas of algebra, including groups. More accessible is [Allenby], which covers the essentials of group theory, and older texts such as [Ledermann] (from which I got the idea of looking at groups of order six) still have much material of interest.

[Allenby] R. B. J. T. Allenby, *Rings, Fields and Groups*, Butterworth–Heinmann, 1991.

[Lang] S. Lang, *Algebra*, Springer–Verlag, 2002.

[Ledermann] W. Ledermann, *Introduction to Group Theory*, Longmans, 1973.

The AGM and a formula for π

Tony Forbes

A long time ago I was asked to prepare something for an M500 Winter Weekend as an emergency backup in case the regular presenter suddenly became unavailable. Fortunately that never happened. However, the work was not wasted and indeed much later saw light at a talk for the London South Bank University Mathematics Study Group on 14th March 2012, a date that seems appropriate for material concerning the computation of π. This was Pi-day—in the USA March 14th is often written as 3.14. As this stuff was originally prepared for M500 members I thought it would be a good idea to present it here. I'm slightly uncertain about the origin of the material. Most likely it was inspired by the book *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity* by J. M. Borwein & P. B. Borwein. The AGM in the title is short for the arithmetic–geometric mean.

Start with two numbers, a and b. Compute the arithmetic mean, $(a+b)/2$, and call it a_1. Compute the geometric mean, $\sqrt{ab}$, and call it b_1. Do it again with a_1 and b_1 to get a_2 and b_2. And again, ... In general, for any a, b,

$$\begin{aligned} a_0 &= a, & b_0 &= b, \\ a_{n+1} &= \frac{a_n + b_n}{2}, & b_{n+1} &= \sqrt{a_n b_n}. \end{aligned}$$

It can be shown that for any starting values (a, b), this process converges to a common limit, called the *arithmetic–geometric mean* of a and b. The main purpose of what follows is to investigate an interesting connection between the AGM and a very efficient formula for computing π to great accuracy.

Hereafter we denote the AGM of a and b by

$$A(a,b) = a_\infty = b_\infty.$$

Thus $a_n \to A(a,b)$ and $b_n \to A(a,b)$ as $n \to \infty$.

For example, $A(0,0) = A(0,1) = A(1,0) = 0$, $A(1,1) = 1$, $A(1,2) \approx 1.45679$, $A(1,3) \approx 1.86362$, $A(1,1000) \approx 189.388$. More generally, one can prove that

$$A(0,a) = A(a,0) = 0, \quad A(a,a) = a.$$

and that

$$A(a,b) = A\left(\frac{a+b}{2}, \sqrt{ab}\right).$$

Let

$$L(a,b) \;=\; \frac{2}{\pi}\int_0^\infty \frac{dx}{\sqrt{(x^2+a^2)(x^2+b^2)}}. \tag{1}$$

Making the substitution $x = b\tan\theta$, $dx/d\theta = b\sec^2\theta$ to transform this integral to

$$L(a,b) \;=\; \frac{2}{\pi}\int_0^{\pi/2} \frac{d\theta}{\sqrt{a^2\cos^2\theta + b^2\sin^2\theta}},$$

we see almost immediately that

$$L(a,a) \;=\; \frac{1}{a}. \tag{2}$$

Moreover, by applying the substitution $u = \dfrac{x}{2} - \dfrac{ab}{2x}$, $\dfrac{du}{dx} = \dfrac{1}{2} + \dfrac{ab}{2x^2}$ to the integral in (3), below, one can verify that

$$L(a,b) \;=\; \frac{1}{\pi}\int_{-\infty}^{\infty} \frac{du}{\sqrt{\left(u^2 + \left(\dfrac{a+b}{2}\right)^2\right)\left(u^2 + \left(\sqrt{ab}\right)^2\right)}}. \tag{3}$$

Hence

$$L(a,b) \;=\; L\left(\frac{a+b}{2}, \sqrt{ab}\right). \tag{4}$$

So, if a_n and b_n are defined as above, (4) implies

$$L(a_{n+1}, b_{n+1}) \;=\; L(a_n, b_n).$$

Therefore

$$L(a,b) \;=\; L(a_1,b_1) \;=\; L(a_2,b_2) \;=\; \ldots \;=\; L(a_\infty, b_\infty) \;=\; L(A(a,b), A(a,b)).$$

It looks as if the function L has the same kind of effect on (a,b) as A. Thus if $m = A(a,b)$,

$$L(a,b) \;=\; L(m,m) \quad \text{and} \quad A(a,b) \;=\; A(m,m).$$

Combining with $L(a,a) = \dfrac{1}{a}$ from (2) and $A(a,a) = a$, this must mean that for any a, b,

$$L(a,b) \;=\; \frac{1}{A(a,b)}. \tag{5}$$

Let us pause and reflect. We started off by defining a simple arithmetic process which converts a pair of numbers to a single number by a kind of limiting process. All fairly straightforward so far. Then we defined a hideous looking integral and after a couple of transformations we have proved that the integral and the AGM process are closely related—the one is the reciprocal of the other. Indeed, the more you think about it, the more amazing equality (5) becomes.

Instead of $L(a, b)$ we will work with a related integral. Let $0 < u < 1$ and let $v = \sqrt{1 - u^2}$. Then $u^2 + v^2 = 1$ and $\dfrac{dv}{du} = -\dfrac{u}{v}$.

The *complete elliptic integral of the first kind* is defined by

$$K(u) \;=\; \int_0^{\pi/2} \frac{d\theta}{\sqrt{1 - u^2 \sin^2 \theta}}. \tag{6}$$

Clearly

$$\frac{1}{A(1, u)} \;=\; L(1, u) \;=\; \frac{2}{\pi} K\left(\sqrt{1 - u^2}\right) \;=\; \frac{2}{\pi} K(v)$$

and, by differentiating (6) with respect to u,

$$K'(u) \;=\; \frac{dK(u)}{du} \;=\; \int_0^{\pi/2} \frac{u \sin^2 \theta \, d\theta}{(1 - u^2 \sin^2 \theta)^{3/2}}. \tag{7}$$

Henceforth we will consider the AGM process with starting values 1 and u, where u is a variable. Now consider a_n and b_n as functions of u: $a_n(u)$ and $b_n(u)$. Thus

$$a_0(u) = 1, \qquad b_0(u) = u,$$

$$a_{n+1}(u) = \frac{a_n(u) + b_n(u)}{2}, \qquad b_{n+1}(u) = \sqrt{a_n(u)\, b_n(u)}.$$

Since $a_n(u)$ and $b_n(u)$ are functions of u they can be differentiated. For brevity we write

$$a_n'(u) \;=\; \frac{d}{du} a_n(u), \qquad\qquad b_n'(u) \;=\; \frac{d}{du} b_n(u).$$

Then

$$a_1(u) = \frac{1 + u}{2}, \quad b_1(u) = \sqrt{u},$$

$$a_0'(u) = 0, \quad b_0'(u) = 1, \qquad a_1'(u) = \frac{1}{2}, \quad b_1'(u) = \frac{1}{2\sqrt{u}}$$

and

$$\begin{aligned} a'_{n+1}(u) &= \frac{a'_n(u)+b'_n(u)}{2}, \\ b'_{n+1}(u) &= \frac{a'_n(u)\sqrt{\dfrac{b_n(u)}{a_n(u)}}+b'_n(u)\sqrt{\dfrac{a_n(u)}{b_n(u)}}}{2}. \end{aligned}$$

Recalling that $v=\sqrt{1-u^2}$, $\dfrac{dv}{du}=-\dfrac{u}{v}$ and

$$\lim_{n\to\infty} a_n(u) = \lim_{n\to\infty} b_n(u) = A(1,u) = \frac{\pi}{2K(v)}, \tag{8}$$

differentiate with respect to u to get

$$\lim_{n\to\infty} a'_n(u) = \lim_{n\to\infty} b'_n(u) = \frac{\pi\ u\ K'(v)}{2\ v\ K^2(v)}. \tag{9}$$

Now let

$$x_n = \frac{a_n(u)}{b_n(u)}, \qquad y_n = \frac{b'_n(u)}{a'_n(u)}, \qquad \pi_n = \sqrt{8}\ \frac{b^2_{n+1}(u)\ a_{n+1}(u)}{a'_{n+1}(u)}.$$

Using the formulae for a_{n+1}, b_{n+1}, a'_{n+1} and b'_{n+1}, we see that

$$\begin{aligned} x_{n+1} &= \frac{\sqrt{x_n}+\dfrac{1}{\sqrt{x_n}}}{2}, \quad y_{n+1} = \frac{y_n\sqrt{x_n}+\dfrac{1}{\sqrt{x_n}}}{y_n+1}, \\ \pi_{n+1} &= \pi_n\ \frac{x_{n+1}+1}{y_{n+1}+1}. \end{aligned} \tag{10}$$

From now on we fix the value of the variable u. Let $u=1/\sqrt{2}$. Then $v=1/\sqrt{2}$, $a_0(u)=1$, $b_0(u)=1/\sqrt{2}$, $x_0(u)=\sqrt{2}$, $y_0(u)=\infty$,

$$x_1 = \frac{2^{1/4}+2^{-1/4}}{2}, \quad y_1 = 2^{1/4} \quad \text{and} \quad \pi_0 = 2+\sqrt{2}.$$

Using (8), (9) and the definition of π_n, we have

$$\pi_n \to \frac{\pi^2}{\sqrt{2}\ K(1/\sqrt{2})\ K'(1/\sqrt{2})} \qquad \text{as} \quad n\to\infty.$$

Then from the 'well-known' formula (see page 18)

$$\int_0^{\pi/2}\int_0^{\pi/2} \frac{\sin^2\phi\; d\phi\; d\theta}{(2-\sin^2\theta)^{1/2}\;(2-\sin^2\phi)^{3/2}} \;=\; \frac{\pi}{4},$$

together with (6) and (7), we obtain

$$\sqrt{2}\; K(1/\sqrt{2})\; K'(1/\sqrt{2}) \;=\; \pi,$$

and finally we have the result that we have been aiming for:

$$\pi_n \;\to\; \pi \qquad \text{as} \quad n \to \infty.$$

Traditionally, if you wanted to calculate π to great accuracy, you would have probably used one of those arctangent formulae, such as Machin's:

$$\pi \;=\; 16\arctan\frac{1}{5} - 4\arctan\frac{1}{239}.$$

When combined with the arctan series,

$$\arctan x \;=\; x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots,$$

this gives a rapidly converging series for π. However, it is only a simple power-series and as such the number of decimal places of π delivered by that formula depends no better than linearly on the number of terms used in the summation.

Contrast with calculating an algebraic number, α, say. We find a polynomial equation satisfied by α, say $P(x) = 0$, and we use the Newton–Raphson method. That is, we guess a first approximation, α_0 and then do

$$\alpha_{n+1} \;=\; \alpha_n - \frac{P(\alpha_n)}{P'(\alpha_n)}$$

for $n = 0, 1, \ldots$. Take $\sqrt{m}$ for instance. Then $P(x) = x^2 - m$ and the recursive part of the Newton–Raphson algorithm becomes

$$\alpha_{n+1} \;=\; \frac{\alpha_n}{2} + \frac{m}{2\alpha_n}.$$

With $m = 2$ and $\alpha_0 = 1$ as initial guess, 15 iterations are enough for 20000-digit accuracy.

As you can see, in general a recursive algorithm is much better than summing a power series. However, π is not algebraic. So the Newton–Raphson method is not available. On the other hand, the algorithm we have developed, namely (10) together with the starting values,

$$x_1 \;=\; \frac{2^{1/4}+2^{-1/4}}{2}, \qquad y_1 \;=\; 2^{1/4} \qquad \text{and} \qquad \pi_0 \;=\; 2+\sqrt{2}, \tag{11}$$

is recursive. And to give some idea how fast it is, starting with (11), only 12 iterations of (10) are needed for 20000 decimal place accuracy.

With a computer equipped with suitable multi-precision software, you can use (11) together with (10), to write a simple program that quickly computes π to thousands of decimal places. For example, if you have MATHEMATICA, try running this code and verify that the result agrees with the true value of π to at least 20000 decimal places.[1]

```
p = 20020;      (* Set precision to 20020 places *)
y = Sqrt[Sqrt[2]];                                          (* y1 *)
x = (Sqrt[Sqrt[2]] + 1/Sqrt[Sqrt[2]])/2;                    (* x1 *)
pi = (2 + Sqrt[2])(x + 1)/(y + 1);                          (* π1 *)
Do[y = N[(y Sqrt[x] + 1/Sqrt[x])/(y + 1), p];               (* yn+1 *)
   x = N[(Sqrt[x] + 1/Sqrt[x])/2, p];                       (* xn+1 *)
   pi = N[pi (x + 1)/(y + 1), p],                           (* πn+1 *)
   {n, 1, 12}]                  (* Loop 12 times *)
```

```
3.14159265358979323846264338327950288419716939937510582097494459230781640628620899862803482534211706 79
82148086513282306647093844609550582231725359408128481117450284102701938521105559644622948954930381 96
44288109756659334461284756482337867831652712019091456485669234603486104543266482133936072602491412 73
72458700660631558817488152092096282925409171536436789259036001133053054882046652138414695194151160 94
33057270365759591953092186117381932611793105118548074462379962749567351885752724891227938183011949 12...
```

Alternatively, you can use this algorithm to construct possible candidates for circle squaring. The starting values as well as the iterations are ruler-and-compasses constructible; hence so is π_n for all positive integers n. For example,

$$\pi_2 \;=\; \frac{\left(2+\sqrt{2}\right)\left(4+2\sqrt[4]{2}+2^{3/4}\right)\left(2\sqrt[8]{2}+2^{5/8}+2\cdot 2^{7/8}+4\sqrt{2+\sqrt{2}}\right)}{8\left(2\left(1+\sqrt[4]{2}\right)\sqrt{2+\sqrt{2}}+2^{3/8}\left(2+3\sqrt{2}\right)\right)},$$

correct to a modest 8 decimals. The precision is more than doubled by the

[1] Some readers might accuse me of cheating because I am blatantly using MATHEMATICA's on-board square root function. However, this is not a serious issue. There would be no significant loss of performance if I wrote my own function to compute $\sqrt{m}$ to the necessary precision using the method described on page 16.

next iteration, $\pi_3 = \alpha_3/\beta_3$, where

$$\begin{aligned}
\alpha_3 &= \left(2+\sqrt{2}\right)\left(4+2\sqrt[4]{2}+2^{3/4}\right)\left(2\sqrt[8]{2}+2^{5/8}+2\cdot 2^{7/8}+4\sqrt{2+\sqrt{2}}\right)\\
&\quad\left(4\sqrt[16]{2}\sqrt{2+\sqrt{2}}\right.\\
&\qquad \left.+\,4\sqrt[4]{2+\sqrt{2}}\sqrt{4+2\sqrt[4]{2}+2^{3/4}}+2^{3/16}\left(2+\sqrt{2}+2\cdot 2^{3/4}\right)\right),\\
\beta_3 &= 32\left(2\left(1+\sqrt[4]{2}\right)\left(2+\sqrt{2}\right)^{3/4}\sqrt{4+2\sqrt[4]{2}+2^{3/4}}\right.\\
&\qquad +\; 2^{3/8}\sqrt[4]{2+\sqrt{2}}\left(2+3\sqrt{2}\right)\sqrt{4+2\sqrt[4]{2}+2^{3/4}}\\
&\qquad +\; \left.\sqrt[16]{2}\left(16+12\sqrt[4]{2}+9\sqrt{2}+10\cdot 2^{3/4}\right)\right),
\end{aligned}$$

giving π to about 18 decimal places.

Problem 261.2 – Trigonometric double integral

Show that

$$\int_0^{\pi/2}\int_0^{\pi/2}\frac{\sin^2\phi\,d\phi\,d\theta}{(2-\sin^2\theta)^{1/2}\,(2-\sin^2\phi)^{3/2}} \;=\; \frac{\pi}{4}.$$

Problem 261.3 – Sums of powers

Tony Forbes

(i) Given a positive integer m, find the smallest positive integer n such that

$$1^m+2^m+\cdots+(n-1)^m \;\ge\; n^m.$$

For example, when $m=2$, $n=5$ since $30=1^2+2^2+3^2+4^2\ge 5^2=25$ whereas $1^2+2^2+3^2<4^2$, $1^2+2^2<3^2$ and $1^2<2^2$. This might or might not be closely related to another problem, suggested to me by Robin Whitty.

(ii) Show that for any positive integer m,

$$1^m+2^m+\cdots+(m-1)^m \;<\; \frac{m^m}{e-1} \;\approx\; 0.581977\,m^m. \qquad (1)$$

Also show that you cannot replace $e-1$ by a larger number, in the sense that (1) would fail for some integer m if you did.

Solution 258.6 – Kolmogorov Distance

Kolmogorov Distance is a non-parametric test of the similarity of two statistical distributions. Kolmogorov Distance is the maximum separation in the y axis between the CDFs under test. Prove that the x coordinate of this maximum separation is where the PDFs of the two distributions cross.

Tony Forbes

If we assume the CDFs are appropriately well behaved, once we unravel the wording of the problem we find that there is a straightforward answer. Suppose the distributions have differentiable CDFs $C_1(x)$ and $C_2(x)$, say, with corresponding PDFs $P_1(x)$ and $P_2(x)$. Recall that $P_i(x) = dC_i(x)/dx$. Then the maximum separation in the y axis between the CDFs will occur at a point where $d(C_1(x)-C_2(x))/dx = 0$; that is, where $P_1(x)-P_2(x) = 0$.

On the other hand, things seem to go wrong (at least sometimes) if the PDFs are discrete, as the following example shows.

x	1	2	3	4	4	6	7	8	9	10
$20P_1(x)$	1	1	2	2	4	4	2	2	1	1
$20P_2(x)$	1	2	3	3	3	3	3	1	1	0
$20C_1(x)$	1	2	4	6	10	14	16	18	19	20
$20C_2(x)$	1	3	6	9	12	15	18	19	20	20
$20\lvert C_1(x) - C_2(x)\rvert$	0	1	2	3	2	1	2	1	1	0

So a further problem is suggested. What's gone wrong?

Equation

Vincent Lynch

Rearrange this equation to produce a seasonal message:

$$y \;=\; \frac{\log(x/m - sa)}{r^2}.$$

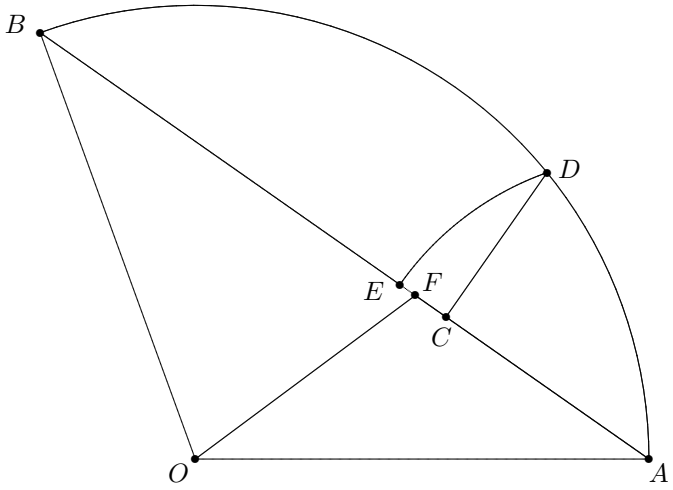
(See somewhere else in this magazine for the answer.)

Problem 261.4 – Projectile

A projectile is fired from a cannon in a uniformly distributed random direction above the ground. Show that the probability of it exceeding a fraction α of its maximum range is $\sqrt{1-\alpha}$. As usual, air resistance is non-existent, the ground is flat and gravity acts vertically downwards.

Problem 261.5 – Angle Trisection

The diagram represents a Euclidean construction due to Albrecht Dürer for trisecting an angle—at least approximately—if the angle is not too large. Angle $AOB = \theta$, $|AC| = |AB|/3$, angle $ACD = 90°$, $|AE| = |AD|$ and $|EF| = |EC|/3$. Find an exact expression for $\angle AOF$ as a function of θ.



Problem 261.6 – Determinant equation

Solve

$$\begin{vmatrix} x & 1 & 2 & 3 & 4 & 5 \\ 5 & x & 1 & 2 & 3 & 4 \\ 4 & 5 & x & 1 & 2 & 3 \\ 3 & 4 & 5 & x & 1 & 2 \\ 2 & 3 & 4 & 5 & x & 1 \\ 1 & 2 & 3 & 4 & 5 & x \end{vmatrix} = 0.$$

Problem 261.7 – Integrals involving roots

Let a and b be positive integers. Compute

$$\int_0^1 \left(1 - x^{1/a}\right)^{1/b} dx$$

and hence show that it is rational.

M500 Mathematics Revision Weekend 2015

The **M500 Revision Weekend 2015** will be held at

Yarnfield Park Training and Conference Centre,

Yarnfield, Staffordshire ST15 0NL

between Friday 15th and Sunday 17th May 2015.

The standard cost, including accommodation (with en-suite facilities) and all meals from dinner on Friday evening to lunch on Sunday is £285. The standard cost for non-residents, including Saturday and Sunday lunch, is £170. There will be an early booking period up to the 16th April with a discount of £20 for both members and non-members.

Members may make a reservation with a £25 deposit, with the balance payable at the end of February. Non-members must pay in full at the time of application and all applications received after the 28th February must be paid in full before the booking is confirmed. Members will be entitled to a discount of £15 for all applications.

A shuttle bus service will be provided between Stone station and Yarnfield Park on Friday and Sunday. This will be free of charge, but seats will be allocated for each service and must be requested before 1st May. There is free on-site parking for those travelling by private transport.

For full details and an application form see the Society's web site at www.m500.org.uk.

The Weekend is open to all Open University students, and is designed to help with revision and exam preparation. We expect to offer tutorials for most undergraduate and postgraduate mathematics OU modules, subject to the availability of tutors and sufficient applications.

Problem 261.8 – Sin integral

Show that for positive integer n,

$$\int_0^\infty \frac{(\sin x)^{2n-1}}{x}\,dx \;=\; \int_0^\infty \frac{(\sin x)^{2n}}{x^2}\,dx.$$

Answer to page 19:

$$y \;=\; \frac{\log(x/m - sa)}{r^2} \;\Rightarrow\; yr^2 = \log\left(\frac{x}{m} - sa\right) \;\Rightarrow\; me^{yr^2} \;=\; x - sam,$$

$$me^{rry} \;=\; x - mas.$$

04.01

Front cover: Four spheres: See M500 **262** for explanation.

Subscription renewal If your M500 Society membership expires at the end of 2014, you will receive a subscription renewal form either separately by email or, if you do not have an email address, on paper together with this magazine. Please follow the instructions on the form to renew your subscription.