James Cook Mathematical Notes

Volume 6 Issue number 65

September 1994

Editor and publisher: B. C. Rennie
Address: 66, Hallett Road,
Burnside, SA 5066
Australia.

The James Cook Mathematical Notes has been published in 3 issues per year since 1979, but from now on, with the start of Volume 7, it will be irregular, appearing only when enough contributions are avalable. The history of JCMN is that the first issue (a single foolscap sheet) appeared in September 1975, then others at irregular intervals, to number 17 in November 1978. The issues up to number 31 were produced and sent out free by the Mathematics Department of the James Cook University of North Queensland, of which I was then the Professor. In October 1983 this arrangement was beginning to be unsatisfactory, and I changed to publishing the JCMN myself. This issue (Number 65) brings Volume 6 to its end, and includes the Volume Index.

In October 1992 it had become clear that the paying of subscriptions by readers is an inefficient operation. Bank charges for changing currency and for international transfers, with postage, together absorb most of the initial input of money. Therefore we have abandoned subscriptions as from the beginning of 1993, issue number 60. I ask readers only to tell me every two years if they still want to have JCMN. To those who want to give something in return for the JCMN, I ask them to make a gift to an animal welfare society in their own country. The animals of the world will be grateful and so will I.

Contributors, please tell me if and how you would like your address printed.

JCMN 65, September 1994

CONTENTS

QUESTIONS TO THINK ABOUT (JCMN 64, p.6328)

Shailesh Shirali
(Rishi Valley School, Andhra Pradesh, 517352, India)

Question (1) from this note in the previous issue was about the set S of all positive integers n such that n divides $2^n + 1$. I have a few more results on the question of characterizing the elements of S. Indeed, theorems 4 and 5 below allow us, in principle at least, to enumerate the set completely, so that the question asked in the previous issue can be considered to have been completely answered.

Theorem 1 If $n \in S$ then (i) $3n \in S$ and (ii) $2^n + 1 \in S$.

Both assertions have one-line proofs, as noted in the previous issue.

Theorem 2 If $n \in S$ and k is any divisor of n then $kn \in S$.

Proof Write $2^{kn}+1$ as $(2^n+1)(2^{kn-n} - 2^{kn-2n} + - + \ldots + 1)$ In this factorization, the first factor, 2^n+1, is a multiple of n. In the second factor, note that $2^n \equiv -1 \pmod n$ and therefore $2^n \equiv -1 \pmod k$, so that the second factor is $\equiv 1 + 1 + \ldots + 1 \equiv 0 \pmod k$, since there are k terms. Thus the first factor is a multiple of n and the second is a multiple of k, and so $kn \mid 2^{kn} + 1$.

This is a curious result; it means that S is closed with respect to multiplication of any of its elements by divisors of those elements. Thus, since 3 and 171 are elements of S and $171 = 9 \times 19$, any number of the form $3^a 19^b$ with $a \geq 2$ is an element of S, and so is any number of the form $3^a 163^b$ with $a \geq 4$.

Theorem 3 If $n > 1$ and $n \in S$, then $3 \mid n$.

Proof Obviously n is odd. Let p be the *least* prime divisor of n. Since $2^n \equiv -1 \pmod p$, the congruence
$$2^x \equiv -1 \pmod p$$
has solutions in positive integers. Let t be the least such solution; then n must be an odd multiple of t, and 2t must be

the least positive integral solution of the congruence
$$2^x \equiv 1 \pmod p$$
(This follows because p is prime and so the only square roots modulo p are 1 and -1). From the congruence
$$2^{p-1} \equiv 1 \pmod p$$
it follows that p-1 is a multiple of 2t and therefore of t. Next, note that by the choice of p, n is relatively prime to p-1. Concatenating all these statements into a single string, we obtain the following:
$$t \mid n \quad \text{and} \quad t \mid (p-1) \quad \text{and} \quad \gcd(p-1, n) = 1.$$
From this it follows that t = 1. But this implies that
$$2^2 \equiv 1 \pmod p.$$
and so p = 3. Thus every $n \in S$ with $n > 1$ has 3 as a factor.

Theorem 4 Let $n \in S$ and let m be such that
$$n < m \leq 2^n + 1 \quad \text{and} \quad n \mid m \quad \text{and} \quad m \mid 2^n + 1.$$
Then $m \in S$.
(Note that this theorem is a substantial generalization of the second part of theorem 1)

Proof Let m = kn. Then $2^m + 1 = 2^{kn} + 1$, which is a multiple of $2^n + 1$, which in turn is a multiple of m, by the choice of m. The result follows.

Theorem 5 Let $n \in S$ and $n > 1$. Then there exists an integer t such that
$$1 \leq t < n \quad \text{and} \quad t \mid n \quad \text{and} \quad n \mid 2^t + 1.$$
Proof We argue as in theorem 3 above. Since $2^n \equiv -1 \pmod n$, the congruence $2^x \equiv -1 \pmod n$ has positive integral solutions. Let t be the least such solution. Then n must be an odd multiple of t and also, by the choice of t, $n \mid 2^t + 1$. Next, note (as in theorem 3) that 2t must be the least positive integral solution of the congruence
$$2^x \equiv 1 \pmod n,$$
so $2t \mid \varphi(n)$, by Euler's theorem. Also, $\varphi(n) \leq n - 1$, so it follows that $t \leq (n-1)/2 < n$. Thus the integer t has the required property.

Theorem 5 shows that a recursive application of theorem 4 will generate all the elements of S. The following table sets out the results of the recursion. We build up the table row by row, entering new elements in the first column as and when they are generated in the third column.

n	$2^n + 1$	New elements of S, i.e. integers m such that $n < m \le 2^n + 1$, $n \mid m$ and $m \mid 2^n + 1$
1	3	3
3	9	9
9	513	$9 \times 3 = 27$, $9 \times 19 = 171$, 513
27	134217729	$27 \times 3 = 81$, $27 \times 19 = 513$ $27 \times 3 \times 19 = 1539$ $27 \times 87211 = 2354697$ $27 \times 3 \times 87211 = 7064091$ $27 \times 19 \times 87211 = 44739243$ $27 \times 3 \times 19 \times 87211 = 134217729$
81	....	....
171	....	....

Since $2^{81} + 1 = 2417851639229258349412353$, which has the factorization $3^5 \times 19 \times 163 \times 87211 \times 135433 \times 272010961$, we see that the following numbers too are elements of S:

81×3, 81×19, 81×163, 81×87211, 81×135433, ...

Note the presence of the primes

3, 19, 163, 87211, 135433, ...

An obvious question: what primes occur in this list?

HERMITEAN MATRICES (JCMN 64, p.6342)

Terry Tao
(Mathematics Department, Princeton Univ. NJ 08544, USA)

A and B are invertible Hermitean matrices; if their arithmetic and harmonic means are both positive definite, does it follow that A and B are both positive definite?

YES

Proof Since the sum A+B is positive definite there exists a positive definite Hermitean matrix C with square equal to A+B.

Let $X = C^{-1}AC^{-1}$, and $Y = C^{-1}BC^{-1}$.

Note that if P is Hermitean then so are CPC and $C^{-1}PC^{-1}$, and if P is positive definite then so are CPC and $C^{-1}PC^{-1}$. (Proof: for any column vector v with Hermitean conjugate v*, consider $v^*CPCv = (Cv)^*P(Cv) > 0$).

Thus X and Y are both Hermitean, and their sum is $X + Y = C^{-1}(A + B)C^{-1} = C^{-1}C^2C^{-1} = I$. Secondly, $X^{-1} + Y^{-1} = C(A^{-1} + B^{-1})C$ is positive definite.

Note that $X^{-1} + Y^{-1} = (X - X^2)^{-1}$, and therefore $X - X^2$ is also positive definite, and all its eigenvalues are positive. Let λ be any eigenvalue of X (we know that it is real because X is Hermitean), then $\lambda - \lambda^2 > 0$, and therefore $0 < \lambda < 1$, which proves that X and Y are positive definite, for $1 - \lambda$ is an eigenvalue of Y if and only if λ is an eigenvalue of X.

Finally, A = CXC and B = CYC are positive definite.

THE DREADED ZETA THREE AGAIN

C. J. Smyth
(Mathematics Department, University of Edinburgh)

It seems empirically that

$$\sum_{n=1}^{\infty} n^{-2} \sum_{m=1}^{n} 1/m = 2 \sum_{n=1}^{\infty} 1/n^3 = 2\zeta(3)$$

Can this equation be proved?

We can prove that

$$\sum_{n=1}^{\infty} n^{-3} \sum_{m=1}^{n} 1/m = \frac{5}{4}\zeta(4) = \pi^4/72$$

CONGRATULATIONS

Nigel Tao at the International Mathematical Olympiad in Hong Kong in July 1994 won a bronze medal.

QUOTATION CORNER 48

For to be possessed of a vigorous mind is not enough; the prime requisite is rightly to apply it.

—— René Descartes, *Discourse on Method* (translation by John Veitch)

BINOMIAL IDENTITY 38 (JCMN 64, p.6342)

$$\sum_{r=1}^{n} (-1)^{n-r}\binom{n}{r}\binom{mr}{n+1} = nm^n(m-1)/2.$$

Each side of the equation is the number, N, of ways of choosing n + 1 of the mn elements in a rectangular $m \times n$ array of m rows and n columns, so that at least one element in each column is chosen.

Consider the left hand side of the equation above. Write it as $\Sigma(-1)^{n-r}c_r$, it will be seen that c_n is the number of ways of choosing n+1 elements unconditionally. More generally, $c_r = \binom{n}{r}\binom{mr}{n+1}$ is the number of ways in which we can firstly choose n-r columns to be excluded, and then choose n+1 elements from anywhere in the remaining r columns. The inclusion-exclusion principle tells us that the number of ways in which the choice can be made with at least one chosen element in each column is

$$N = c_n - c_{n-1} + c_{n-2} - \ldots\ldots$$

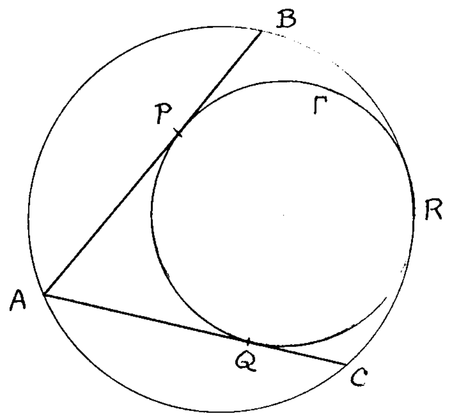
Now we shall calculate the total number N in a different way. A choice of the kind required gives two elements in one column, and one in each of the other columns. Suppose that of the two elements in one column we label one as "first" and the other as "second"; there are 2N ways of choosing such an arrangement. But to make such a choice we need to choose one element in each column (which we can do in m^n ways) and then choose (in n ways) one of the columns to have a "second" element, and then choose (in m-1 ways) where to have the "second" element in the chosen column. Therefore

$$2N = m^n n(m-1),$$

so that N = the right hand side of the equation above.

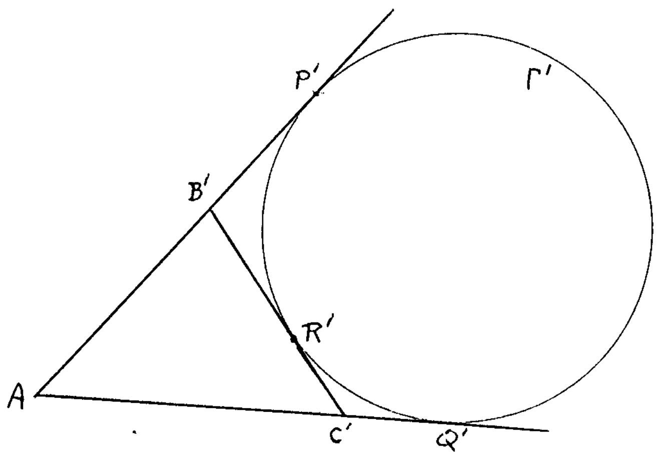
SECOND TRIANGLE PROBLEM (JCMN 64 p.6338)

Shailesh Shirali and Sahib Ram Mandan



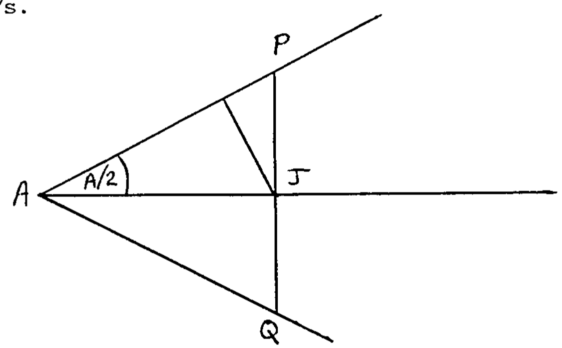
The problem in JCMN 64 (contributed by Shailesh Shirali, but also suggested by Sahib Ram Mandan) was to show that the mid-point of PQ is the incentre I of the triangle ABC in the figure above.

<u>First Proof</u>: Invert the figure from the vertex A, using the radius $\sqrt{bc}$. Denote the image of B by B′, etc.



The triangle AB′C′ is congruent to ACB (because AB′ = bc/AB = b = AC, and AC′ = bc/AC = c = AB). The image of the

circumcircle is the line B′C′, and the image of the circle Γ is a circle Γ′ touching AB′ at P′, AC′ at Q′ and B′C′ at R′, it is an escribed circle of the triangle AB′C′, so that AP′ = AQ′ = s = (a+b+c)/2. Therefore in the original figure AP = AQ = bc/s.

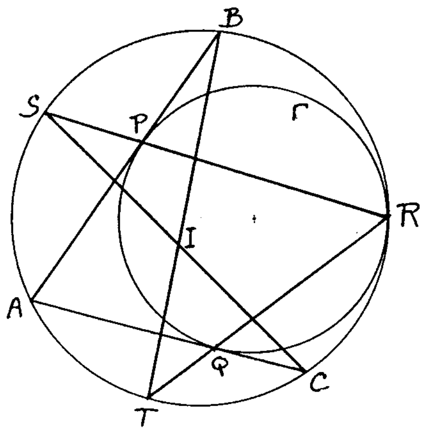


Denote the mid-point of PQ by J. The perpendicular distance from J to AB or AC is:

$$PJ \cos \tfrac{1}{2}A = AP \cos \tfrac{1}{2}A \sin \tfrac{1}{2}A = \tfrac{1}{2}(bc/s)\sin A = \Delta/s$$

(where Δ is the area of the triangle ABC), which is the in-radius of ABC. Because J is on the bisector of the angle at A, it follows that J is I.

<u>Second Proof</u> Use the result of the TRIANGLE PROBLEM in JCMN 64, that (in the figure below) CI meets RP at S and BI meets RQ at T, both on the circumcircle. Apply Pascal's theorem to the hexagon RSCABT. The intersections P, I and Q of opposite sides are collinear, establishing our result.

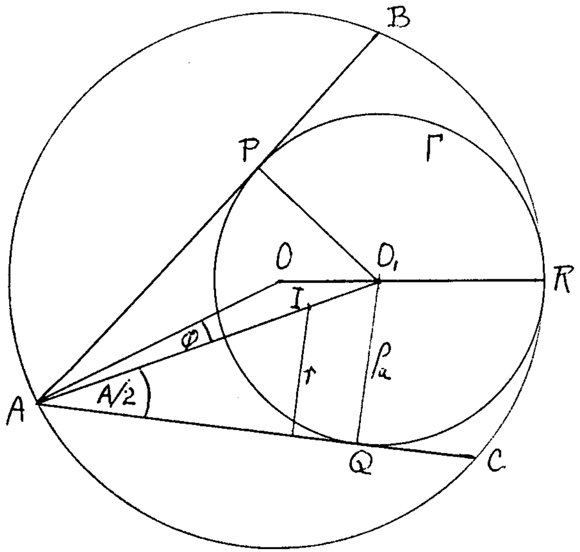


SECOND TRIANGLE PROBLEM AGAIN

Jordan Tabov has sent a copy of a 1991 article by Vesselin Nenchev (Веселин Ненчев) of Beli Osam (Бели Осъм) about triangle geometry, giving several results, including essentially a solution to this problem from JCMN 64.

The calculation starts with the equation $OI = \sqrt{R(R-2r)}$ giving the distance from the circumcentre O to the incentre I in terms of the circumradius R and inradius r.

From this value for the length OI it is possible to calculate the angle φ in the drawing below.

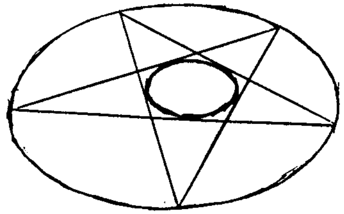


$$\cos\varphi = \frac{r + R(1 - \cos A)}{2R\sin(A/2)}$$

Denoting the radius of the circle Γ by ρ_a, we have three sides and one angle of the triangle AOO_1, and by the cosine rule we get an equation, $\rho_a = 2r/(1 + \cos A) = r/\cos^2 A/2$. This tells us that I is on PQ.

POLYGON PROBLEM

Poncelet's Porism (often called the porism of the inscribed and circumscribed polygon) tells us that if there are two conics and if a polygon has all its vertices on one conic and all its edges touching the other, then there are infinitely many other polygons (of the same number of sides) with the same property.

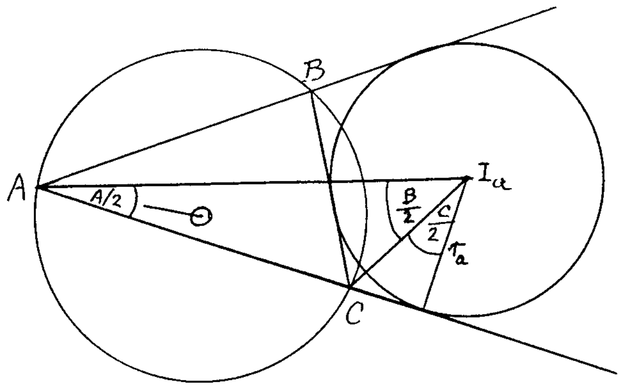


It is a theorem in projective geometry, and so it is equivalent to the proposition with "circles" instead of "conics". We can therefore express the theorem as:

Given any n, if two circles are such that one n-gon has all its vertices on one circle and all its sides touching the other, then there are infinitely many n-gons with the same property.

The simplest non-trivial case is n = 3. If we start with any triangle, with in-radius = r and circum-radius = R (where R > 2r) and with the centres of the incircle and circumcircle at distance d apart, then 2Rr = (R+d)(R-d). Conversely, any two circles with these properties are the inscribed and circumscribed circles of some triangle, and therefore also of infinitely many other triangles.

But the circumcircle and one of the escribed circles of any triangle also form a pair of circles with the required property of having a triangle with vertices on one and sides touching the other. The relation between their radii and their centre distance may be found as follows:



Comparing two calculations for twice the area of the triangle AI_aC, we find $(r_a/\sin A/2)(r_a/\cos C/2)\sin B/2 = br_a = 4Rr_a \sin B/2 \cos B/2$, and $r_a = 4R \sin A/2 \cos B/2 \cos C/2$, The angle I_aAO is $(B-C)/2$ in the diagram above, and the length AI_a is $r_a/\sin A/2 = 4R \cos B/2 \cos C/2$.

By the cosine rule

$$d^2 = R^2 + 16R^2 \cos^2 B/2 \cos^2 C/2 - 8R^2 \cos B/2 \cos C/2 \cos \frac{B-C}{2},$$

$$d^2 - R^2 = 8R^2 \cos B/2 \cos C/2 \left(2 \cos B/2 \cos C/2 - \cos \frac{B-C}{2}\right)$$

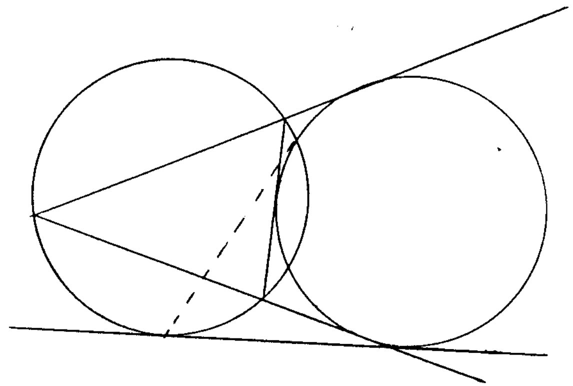
$$= 2Rr_a.$$

Consider the general question: If an n-gon has all its vertices on a circle of radius R and all its edges touching a circle of radius r, then what condition must R, r and the centre distance d satisfy?

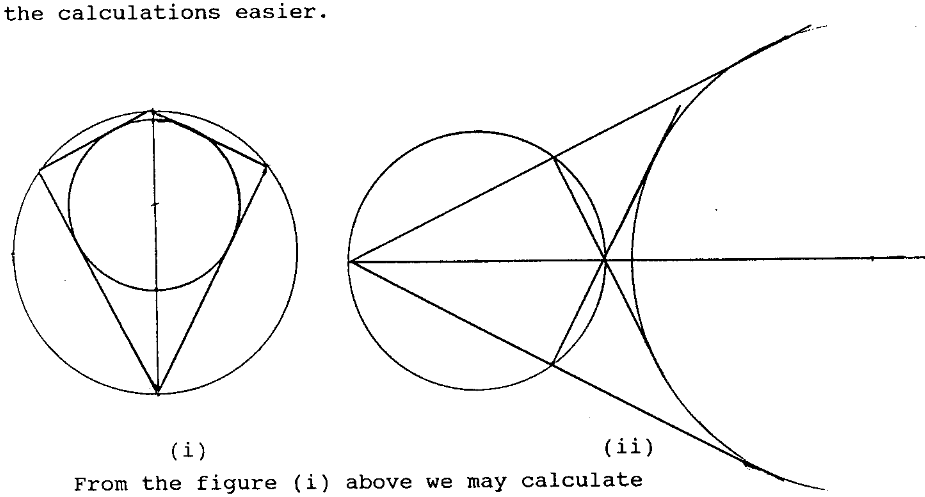
For $n = 3$ we have found the answer: $R^2 = d^2 \pm 2Rr$.

The ideas above suggest a geometrical problem:

The figure below shows any triangle ABC with its circumcircle and one of its escribed circles. Show that the tangent to the escribed circle at the intersection of the two circles will meet the circumcircle again at a point of contact of a common tangent to the two circles.



Now return to the inscribed and circumscribed polygons associated with two circles. What about $n = 4$? Consider the figures below, they are chosen to be symmetrical to make the calculations easier.



(i) (ii)

From the figure (i) above we may calculate

$$R^2 = d^2 + r\sqrt{(2R^2 + 2d^2)}$$

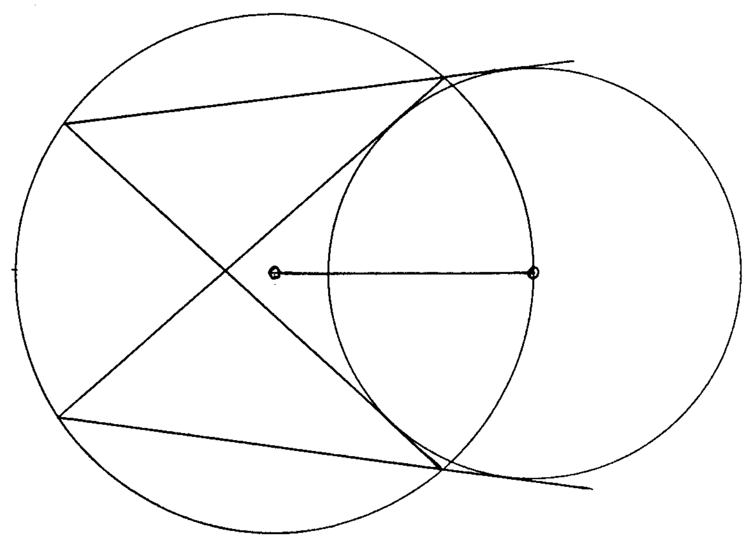
and from (ii) almost the same equation, in this case $d > R$,

$$R^2 = d^2 - r\sqrt{(2R^2 + 2d^2)}.$$

Both equations may be written $R^4 + d^4 = 2R^2d^2 + 2d^2r^2 + 2r^2R^2$.

Is there any other possible configuration leading to a different equation for the case of $n = 4$?

Yes there is! If $R = d$ the construction is possible, for any $r < 2R$, as may be seen from the drawing below.



YEAST MIXING

This is a model for what might happen in making bread. The yeast is a fine powder suspended in a fluid which may be thought of as water, though in fact it is a mixture containing milk, sugar and other additives. This yeast mixture is initially at a temperature of 0°; the scale of temperature is not relevant though you may like to think of it as on the Réaumur scale. Yeast is inactive when cold, and for it to work in the bread dough we want it to be at 20°. To accomplish this we mix three parts of the cold yeast mixture with one part of boiling water at 80°, stirring them together. Assume that there is no conduction of heat, the hot and cold fluids mix by diffusion. It is an unfortunate fact that yeast is killed by temperatures over 40°. What proportion of our original yeast will be killed in the mixing process?

POWER MEAN INEQUALITY (JCMN 42, p.5020)

This problem, from Dmitry Mavlo, was in JCMN 42, p. 5020, in February 1987.

Let x be a vector of non-negative components $(x_1, x_2, \ldots, x_n)$, and denote the vector $(x_1^k, \ldots, x_n^k)$ by x^k. Write A and Γ for the arithmetic and geometric means respectively. Prove that

$$A^k(x) - \Gamma^k(x) \geq n^{1-k}(A(x^k) - \Gamma(x^k)) \quad \ldots\ldots \quad (1)$$

for positive integer k. Find the cases of equality.

We have not yet had a solution sent in, but some progress can be made. It is sometimes convenient to put (1) in the equivalent form:

$$n^k A^k(x) \geq nA(x^k) + (n^k - n)\Gamma^k(x) \quad \ldots\ldots\ldots \quad (1')$$

<u>Theorem 1</u> The inequality (1) or (1′) holds when $n = 2$.
<u>Proof</u> If $u = \Gamma(x)$ we may write the vector x as $(uy, u/y)$, and the required inequality becomes:

$$(y + 1/y)^k - y^k - y^{-k} \geq 2^k - 2 \quad \ldots\ldots\ldots \quad (2)$$

or
$$\sum_{r=1}^{r=k-1} \binom{k}{r} (y^{k-2r} - 1) \geq 0,$$

and by changing the dummy variable to $k-r$, i.e. reversing the order of the terms in the binomial sum, the LHS becomes

$$\Sigma \binom{k}{r} (y^{2r-k} - 1)$$

and because $y^s + y^{-s} - 2 \geq 0$, the result is established.

It may be noted that there is equality in (2) for all y when $k = 1$ or 2, and for all k when $y = 1$, i.e. $x = (u, u)$.

<u>Theorem 2</u> The inequality (1) holds when $n = 4$.
<u>Proof</u> Take the vector x to be (a, b, c, d)

Theorem 1 may be written in the form

$$(x + y)^k \geq x^k + y^k + (2^k - 2)(xy)^{k/2}$$

and by successive applications of this we find that:

$$(a+b+c+d)^k \geq (a+b)^k + (b+c)^k + (2^k - 2)(a+b)^{k/2}(c+d)^{k/2}$$

$$\geq a^k+b^k+c^k+d^k + (2^k - 2)((ab)^{k/2}+(cd)^{k/2}+(a+b)^{k/2}(c+d)^{k/2})$$

Now use the AM-GM inequality, $x + y \geq 2\sqrt{x}\sqrt{y}$,

$$(a+b+c+d)^k \geq a^k+b^k+c^k+d^k + (2^k-2)(2(abcd)^{k/4} + 2^k(abcd)^{k/4})$$
$$= a^k+b^k+c^k+d^k + (4^k-4)(abcd)^{k/4}$$

or $\quad 4^kA^k(x) \geq 4A(x^k) + 4^k\Gamma^k(x) - 4\Gamma(x^k)$ QED

<u>Theorem 3</u> The inequality (1) holds if n is a power of 2.
<u>Proof</u> The proof is by induction, and it is the obvious generalization of Theorem 2. Let x be the vector of length $2n$ formed by joining end-to-end the vectors u and v, both of length n.

$$2^k A^k(x) = (A(u) + A(v))^k \qquad \text{(now use Theorem 1)}$$
$$\geq A^k(u) + A^k(v) + (2^k - 2)\sqrt{(A^k(u)A^k(v))}.$$

$$(2n)^kA^k(x) \geq n^kA^k(u) + n^kA^k(v) + n^k(2^k-2)\sqrt{(A^k(u)A^k(v))}$$
$$\geq nA(u^k) + nA(v^k) + (n^k-n)(\Gamma^k(u)+\Gamma^k(v))$$
$$+ n^k(2^k-2)\Gamma^{k/2}(u)\Gamma^{k/2}(v) \qquad \text{(by the induction hypothesis)}$$
$$\geq 2nA(x^k) + 2(n^k-n)\Gamma^{k/2}(u)\Gamma^{k/2}(v) + n^k(2^k-2)\Gamma^{k/2}(u)\Gamma^{k/2}(v)$$
$$\geq 2nA(x^k) + (2n^k - 2n + 2^kn^k - 2n^k)\Gamma^k(x)$$
$$\geq 2nA(x^k) + (2^kn^k - 2n)\Gamma^k(x). \qquad \text{QED}$$

Is there a way to extend the proof to values of n that are not powers of 2? A difficulty is that applying the ($n=4$) result to a vector (x, x, y, y) gives an inequality weaker than that obtained by applying the ($n=2$) result to the vector (x, y).

Another problem —— what happens if k is not an integer? Take any $x > 1$ and consider the function

$$(x + 1/x)^k - x^k - x^{-k} + 2 - 2^k$$

We know that it is zero when $k = 1$ or 2. Prove (or disprove) that it is < 0 when $1 < k < 2$ and > 0 when $k > 2$.

RECONSTRUCTING AN EXAM QUESTION

A. Brown
(50/55 Burkitt St., Page, A.C.T. 2614, Australia)

In an article in the American Mathematical Monthly (Vol 101, 1994, 151-161) H. B. Griffith and A. E. Hirst cite a 1910 Higher Certificate examination question:

> Prove that if α, β, γ are the three roots of the equation $x^3 - 21x + 35 = 0$, then $\alpha^2 + 2\alpha - 14$ will be equal to β or γ.

They provide a way of answering the question, and add "The question makes one wonder how the examiner found the numbers in it so that it would work at all". To throw light on this they ask about finding p, q, a, b, c such that if

$$C(x) = x^3 - px + q \quad \text{and} \quad Q(x) = ax^2 + bx + c,$$

and if α is a root of the cubic $C(x) = 0$ then $Q(\alpha)$ is one of the other roots of the cubic.

From the point of view of an examiner, it is desirable to have integer coefficients in C and Q, but not to have the cubic with roots that can be recognised easily. Special cases such as a triple root or a double root present no difficulty, so that we can assume that the roots are real, distinct and non-zero.

At first sight there seem to be eight possibilities — $Q(\alpha) = \beta$ or γ, $Q(\beta) = \gamma$ or α, $Q(\gamma) = \alpha$ or β, but it is easy to check that there are only two distinct cases, exemplified by

(i) $Q(\alpha) = \beta$, $Q(\beta) = \alpha$, $Q(\gamma) = \alpha$,
(ii) $Q(\alpha) = \beta$, $Q(\beta) = \gamma$, $Q(\gamma) = \alpha$.

In case (i), $Q(\beta) = Q(\gamma)$ gives $b = -a(\beta+\gamma) = a\alpha$ and in similar fashion $Q(\alpha) - Q(\beta) = \beta - \alpha$ gives $-a(\alpha + \beta) - b = 1$, and $b + 1 = a\gamma$, so we have

$$\alpha = b/a \qquad \gamma = (1 + b)/a \qquad \beta = -\alpha - \gamma = -(1 + 2b)/a.$$

From these expressions for α, β, γ we can deduce that

$$p = -\beta\gamma - \gamma\alpha - \alpha\beta = (1 + 3b + 3b^2)/a^2$$
$$q = -\alpha\beta\gamma = b(1 + b)(1 + 2b)/a^3$$
$$c = \beta - a\alpha^2 - b\alpha = -(1 + 2b + 2b^2)/a$$

The discriminant of the cubic is

$$\Delta = (\beta-\gamma)^2(\gamma-\alpha)^2(\alpha-\beta)^2 = 4p^3 - 27q^2 = \frac{(2 + 9b + 9b^2)^2}{a^6}$$

For case (ii) we can think of α, β, γ as the elements of a period three solution of the recurrence relation

$$x_{n+1} = Q(x_n) = ax_n^2 + bx_n + c.$$

Note that a shift of origin for x gives a recurrence relation of similar form, so we can assume that $\alpha + \beta + \gamma = 0$. The cubic $(x-\alpha)(x-\beta)(x-\gamma)$ then provides a suitable form for $C(x)$. Thus we have the basic equations

$$a\alpha^2 + b\alpha + c = \beta$$
$$a\beta^2 + b\beta + c = \gamma$$
$$a\gamma^2 + b\gamma + c = \alpha$$

and $C(x)$ is determined if we can use these equations to obtain $p = -(\alpha\beta + \beta\gamma + \gamma\alpha)$ and $q = -\alpha\beta\gamma$, without necessarily finding α, β, γ explicitly. The equations for α, β, γ have cyclic symmetry, so it is convenient to use Σ for cyclic summation over α, β and γ,

e.g. $\Sigma\alpha^2\beta$ denotes $\alpha^2\beta + \beta^2\gamma + \gamma^2\alpha$.

In general, if we write $A = \Sigma\alpha$, $B = \Sigma\alpha\beta$, $D = \alpha\beta\gamma$, we have algebraic identities $\Sigma\alpha^2 = A^2 - 2B$,

$$\Sigma\alpha^3 = 3D + A^3 - 3AB$$
$$\Sigma\alpha^2\beta^2 = B^2 - 2AD$$
$$\Sigma\alpha^4 = A^4 + 4AD + 2B^2 - 4A^2B$$
$$\Sigma(\alpha^2\beta + \alpha\beta^2) = AB - 3D$$

For $A = 0$, $B = -p$ and $D = -q$, these identities become $\Sigma\alpha^2 = 2p$, $\Sigma(\alpha^2\beta+\alpha\beta^2) = 3q = -\Sigma\alpha^3$, $\Sigma\alpha^4 = 2p^2 = 2\Sigma\alpha^2\beta^2$.

By using the basic equations, we can obtain

$$a\Sigma\alpha^2 + b\Sigma\alpha + 3c = \Sigma\beta$$

$$a\Sigma\alpha^3 + b\Sigma\alpha^2 + c\Sigma\alpha = \Sigma\alpha\beta$$

$$a\Sigma\alpha^4 + b\Sigma\alpha^3 + c\Sigma\alpha^2 = \Sigma\alpha^2\beta$$

$$a\Sigma\alpha^2\beta^2 + b\Sigma\alpha\beta^2 + c\Sigma\beta^2 = \Sigma\beta^3$$

and hence

$$2pa + 3c = 0$$

$$3qa = (2b+1)p$$

$$2p^2a - 3bq + 2pc = \Sigma\alpha^2\beta$$

$$ap^2 + b\Sigma\alpha\beta^2 + 2pc = -3q$$

The last two equations, using $\Sigma(\alpha^2\beta + \alpha\beta^2) = 3q$, give

$$3q(1 + b + b^2) = ap^2(2b - 1) + 2pc(b - 1).$$

Hence $p = -3c/(2a)$, $q = (2b + 1)p/(3a) = -(2b + 1)c/(2a^2)$,

and $-2c(1 + 2b)(1 + b + b^2) = ac^2(1 + 2b)$.

If we assume $q \neq 0$, to avoid a zero root for $C(x) = 0$, then $c(2b + 1) \neq 0$ and the conditions become

$$ac = -2(1 + b + b^2),$$

$$p = 3(1 + b + b^2)/a^2,$$

$$q = (1 + 2b)(1 + b + b^2)/a^3.$$

In this case the discriminant is

$$\Delta = 4p^3 - 27q^2 = 81(1 + b + b^2)^2/a^6 = (3p/a)^2.$$

The solutions for cases (i) and (ii) agree with those given by Griffiths and Hirst, who note that in both cases the expression for Δ offers solutions of the Diophantine problem:

Find integers p, q, r for which $4p^3 - 27q^2 = r^2$.

The 1910 exam question is an example of case (ii), with $a = 1$ and $b = 2$, and indeed the simplest way of constructing a problem of this type is to take $a = 1$ and b an integer.

The approach used in this note can be extended by starting from the same recurrence relation and writing down the basic equations for, say, a period four solution, and then working from the basic equations to construct a fourth degree polynomial whose roots are the elements of the period four solution and hence satisfy a cyclic relation of the type considered in case (ii) above.

As an example we could construct the question:

$F(x) = x^4 - 10x^2 + 15x - 5$, $\quad Q(x) = x^2 + 2x - 5$.

Prove that if α, β, γ, δ are the four roots of $F(x) = 0$, then for a suitable ordering of the roots:

$Q(\alpha) = \beta$, $Q(\beta) = \gamma$, $Q(\gamma) = \delta$, $Q(\delta) = \alpha$.

MATRIX INEQUALITY

The following problem, from H. Kestelman, was in JCMN 9 in May, 1977, but we have not yet had a solution.

If a real square matrix M is positive definite (i.e. $x^TMx > 0$ for all real $x \neq 0$), prove that every principal sub-determinant of M is positive. (A principal sub-matrix is one obtained by deleting any subset of the set of rows and deleting the corresponding columns)

Is the converse true?

INDEX - VOLUME 6 (JCMN 54-65) (1991-1994)

A

B

C

D

E

F