Mathematical Spectrum

1998/9 Volume 31 Number 1

- **Mahāvīra: poet and mathematician**
- **Some properties of the number five**
- **A public-key cryptosystem**
- **A problem of Leonardo of Pisa**

A magazine for students and teachers of mathematics
in schools, colleges and universities

MATHEMATICAL SPECTRUM

This is a magazine for students and teachers in schools, colleges and universities, as well as the general reader interested in mathematics. It is published by the Applied Probability Trust, a non-profit-making organisation established in 1963 with the support of the London Mathematical Society. The object of the Trust is the encouragement of study and research in the mathematical sciences.

One volume of *Mathematical Spectrum* is published in each British academic year consisting of three issues, which appear in September, January and May.

Articles published in *Mathematical Spectrum* deal with the entire range of mathematical disciplines (pure mathematics, applied mathematics, statistics, operational research, computing science, numerical analysis, biomathematics). Both expository and historical material may be included, as well as elementary research and information on educational opportunities and careers in mathematics. There are also sections devoted to problems and to mathematics in the classroom, as well as a computer column.

Mahāvīrācārya: the Poet and the Mathematician

MAHESH DUBE

How poetry and mathematics combined in the work of a ninth century Indian mathematician.

Karl Weierstrass is said to have remarked once that 'a mathematician who is not something of a poet as well can never be a complete mathematician'. This test was passed by Āryabhata, Mahāvīrācārya[1] and Bhāskara, all of whom were mathematicians and poets. In Mahāvīra's work we find a rare combination of extraordinary poetic talent and mathematical genius. He possessed the rigour of a mathematician, the imagination of a poet and the creativity of an artist, tuning his poetry on the chords of mathematics and vice versa. In a way he is a unique figure among ancient Indian mathematicians. His great work, written in Sanskrit, was entitled 'Ganita Sāra Sarigraha' (GSS), which means, roughly, a collection of important mathematical concepts and techniques. The following example from it, illustrates his remarkable capacity for the poetic presentation of an algebraic problem (GSS 4/17–21).

Here Mahāvīra describes an exotic spring night where a couple in love recline in a pleasure garden filled with trees laden with flowers and fruits and resonant with the sweet sounds of parrots, cuckoos and bees which were all intoxicated by the honey obtained from the flowers therein. Then, in a lovers' quarrel the lady's necklace is broken and falls to the ground. One third of the pearls in the necklace reached the maid-servant; a sixth fell on the bed, then a half of that fraction, again a half of this last fraction and so on, counting that way six times in all, of the pearls fell on the floor and scattered; and there were found to remain unscattered 1161 pearls. If you know how to work miscellaneous problems on fractions, find out the total number of pearls in the necklace. This can be algebraically expressed as

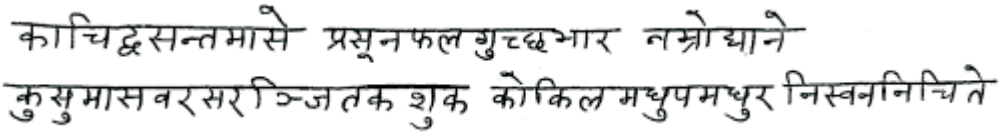
$$\frac{x}{3}+\frac{x}{6}+\frac{x}{12}+\frac{x}{24}+\frac{x}{48}+\frac{x}{96}+\frac{x}{192}+\frac{x}{384}+1161=x,$$

which gives the total number of pearls as 3456.

Very little is known about Mahāvīra and his life. He has written almost nothing about himself. Whatever we could gather, tells us only that he was a contemporary of the Rāstrakūta King Amōghavarsa Nrpatunga in the ninth century, whose patronage he enjoyed in South India, much of what is known as Karnataka today, and that he was a Jain monk.

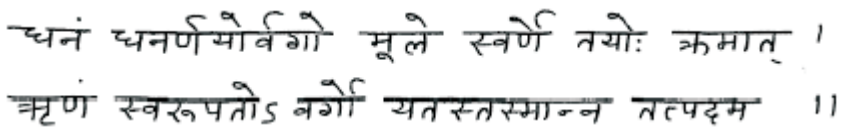
The Rāstrakūta dynasty ruled Southern India for almost two centuries from the second half of the seventh century. In Indian history the Rāstrakūta empire is known for its wider influence, prosperity and political stability. Most of the kings were interested in art, literature and culture. The famous Kailasa temple of Elora is the living monument of Rāstrakūta. It was built in the period 756–773 AD by King Krishna I. Amōghavarsa Nrpatunga ruled (815–877 AD) for almost 62 years. He seems to have been an adherent of the Jainist religion and is known as the author of 'Prasanottar Ratanmālika'. He was also a courageous warrior, a military expert, an able ruler, a literary man and a learned scholar. It was in this period that Mahāvīra flourished and wrote his famous text 'Ganita Sāra Sarigraha'. Written in Sanskrit GSS is the only representative work of Mahāvīra that survives today and which comes to us as authentic. It contains 1100 verses on arithmetic, algebra, geometry and mensuration, and is divided into 9 chapters as follows.

1. Terminology.
2. Arithmetical operations – here rules and examples for multiplication, division, squaring, square roots and cube roots are given.
3. Fractions – here multiplication and division of fractions, summation of fractional series in progression, varieties of fractions, compound and complex fractions are discussed.
4. Miscellaneous problems on fractions.
5. The Rule of Three.
6. Mixed problems.
7. Calculations relating to the measurement of areas.
8. Calculations regarding excavations.
9. Calculations regarding shadows.



GSS 4/17–21.

[1]This is made up of the proper name Mahāvīra and the title ācarya, meaning 'a learned man, scholar or teacher'. Thus Mahāvīrācārya can be translated as 'the learned Mahāvīra'. The shorter form Mahāvīra is the one that is normally employed.



GSS 1/52.

Now we will discuss some of the special features of his mathematical work.

I. Square roots

Mahāvīra explicitly discards the square-root of a negative number (GSS 1/52).

The squares of positive and negative numbers are positive and the square roots of positive numbers are positive and negative. Since there does not exist a number whose square is a negative number, negative numbers do not have square roots. Such a straightforward declaration as early as the ninth century is not only historically important but mathematically significant also. E. T. Bell in his *Development of Mathematics* describes this as 'Mahāvīra's extremely intelligent remark' and writes: 'Mahāvīra had mathematical insight enough to leave the matter there, and not to proceed to meaningless manipulations of unintelligible symbols'. Here Bell not only acknowledges the deep mathematical insight of Mahāvīra, but also praises his mathematical restraint and discipline.

II. Quadratic quations

Mahāvīra knew that a quadratic equation has two roots, but in most of his examples only one root is admissible. The origin of the problems on quadratic equations dates back to the period of the 'Sulva Sutras'[2] in India. The 'Bakshali Manuscript'[3] also suggests that quadratic equations were studied in ancient India. A large number of interesting and descriptive problems on quadratic equations are given by Mahāvīra. Here are some examples.

'One third of a herd of elephants and three times the square root of the remaining part were seen on a mountain slope, and in a lake was seen a tusker (male elephant) along with three female elephants. How many elephants were there?' (GSS 4/41) This gives us the equation

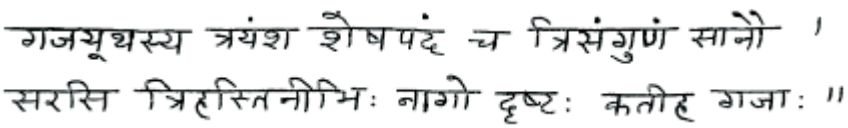
$$\frac{x}{3} + 3\sqrt{\frac{2}{3}x} + 4 = x$$

which can be simplified to

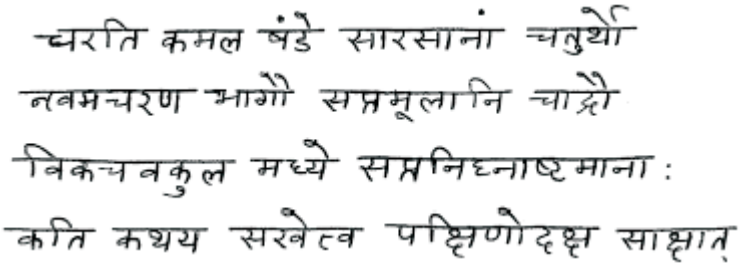
$$(2x - 3)(x - 24) = 0.$$

Accepting only the integral solution we get the number of elephants to be 24.

'One fourth (of an unknown number) of Sārasa birds are seen in the midst of a cluster of lotuses, $\frac{1}{9}$ and $\frac{1}{4}$ parts thereof as well as seven times the square root move on a mountain. Then, in the midst of blossomed vakula trees the remainder is found to be 56 in number. O, you clever friend, tell me exactly how many birds there are altogether.' (GSS 4/36)



GSS 4/41.



GSS 4/36.

[2]Sulva Sutras form a part of the religious texts of the Hindus, where methods for geometrical constructions are described. The word Sulva is derived from the root 'Sulv' which means 'to measure', while Sutra means rules. It is generally believed that these Sulva Sutras were composed in the eighth and ninth centuries before Christ, but some scholars date them to between 500 and 200 BC.

[3]Bakshali is a village near Peshawar in north-west India. The manuscript (discovered in 1881) is an anonymous compendium of rules and examples with their solutions. It is said to belong to the third century AD.

This can be written as

$$\frac{x}{4}+\frac{x}{9}+\frac{x}{4}+7\sqrt{x}+56=x$$

i.e.

$$(x-576)(x-36)=0.$$

Obviously the total number of birds is 576. The value 36 of x is not acceptable since there are more than 56 birds.

In GSS Mahāvīra also discusses the rules for solving equations of higher degree and gives several examples, such as the following.

'Out of a herd of elephants, nine times the square root of a $\frac{2}{3}$rds part of their number and six times the square root of $\frac{3}{5}$th of the remainder (left thereafter), and finally 24 (remaining) elephants with their broad temples wetted with the stream of the exuding ichor, were seen by me in a forest. How many are all the elephants?' (GSS 4/54–55)

If x is the total number of elephants, then we have

$$9\sqrt{\frac{2x}{3}}+6\sqrt{\frac{3}{5}\left(x-9\sqrt{\frac{2x}{3}}\right)}+24=x.$$

Substituting

$$y=x-9\sqrt{\frac{2x}{3}}$$

we have

$$y-6\sqrt{\frac{3}{5}y}=24$$

which gives $y=60$ or $48/5$. Taking $y=60$ we get

$$x-9\sqrt{\frac{2x}{3}}=60$$

i.e. x=150 or 24.

As there are more than 24 elephants the admissible value of $x=150$ gives the total number of elephants. Taking the other value of y we get more non-integral values of x so the solutions are not admissible.

Although Mahāvīra did not discuss the reasons for admissibility and non-admissibility of solutions, he gives several other complex examples noteworthy for repeated use of substitution. Mahāvīra also gives rules for solving simultaneous equations such as

$$\begin{cases}x+y=a,\\ xy=b;\end{cases}$$

and

$$\begin{cases}x^2+y^2=c,\\ xy=b.\end{cases}$$

Mahāvīra also discusses rules for arriving at the gain derived from success and failure in a gambling operation and as an illustration gives the following interesting problem.

द्वित्रिभागस्य यन्मूलं नवघ्न हस्तिनां पुनः
शेष त्रिपंचमांशस्य मूलं षड्भि समाहतम्
विगलद्दानधारार्द्र गण्डमण्डल दन्तिनः
चतुर्विंशतिरादृष्टा मयारण्यां कति द्विपाः

GSS 4/54–55.

दृष्ट्वा कुक्कुटयुद्धं प्रत्येकं तौ च कुक्कुटिकौ
उक्तौ रहस्यवाक्यैर्मन्त्रौषधशक्ति मन्महापुरुषेण
जयति हि पक्षी तेमे देहि स्वर्णं ह्यविजयोऽसि दधांते
तद्द्वित्रयंशकमधेत्यपरं च पुनः स संसृप्य
त्रिचतुर्थं प्रतिवाञ्छत्युभयस्माद् द्वादशैव लाभः स्यात्
तत्कुक्कुटिककरस्थं ब्रूहि त्वं गणकमुख तिलक

GSS 6/270–272.

'A wizard having magical powers sees a cock-fight going on and speaks privately to both the owners of the cocks. To one he says, 'If your bird wins, then you give me your stake-money, but if you lose, I shall pay you two-thirds of it.' Then, going to the other owner, the wizard requires his stake-money if he wins but promises to give him three-fourths of it if he loses. Tell me, O ornament of the first rate mathematicians, the stake-money of each of the cock-owners if, whatever the outcome of the cock-fight, the wizard makes a profit of twelve gold coins.' (GSS 6/270–272) Here let A and B be the two owners and x and y their respective stake-monies. If A wins then the wizard gets x gold coins from A and pays $3/4y$ coins to B. Therefore the wizard's profit is

$$x - \frac{3}{4}y = 12.$$

Similarly, if B wins, then

$$y - \frac{2}{3}x = 12.$$

Solving these two equations we get $x = 42$ and $y = 40$.

III. Geometry

Among the ancient and medieval Indian mathematicians, only Mahāvīra mentions an ellipse which he calls 'āyata vrtta' (elongated circle). He also gives rules for the circumference and area of an ellipse. Although Mahāvīra's formula for the area of an ellipse is not accurate, his rule for the circumference deserves to be mentioned, as it gives a remarkably close approximation. Mahāvīra says:

'The square of the shorter diameter is multiplied by 6 and the square of twice the length (as measured by the longer diameter) is added to this. The square root of this sum gives the measure of the circumference.' (GSS 7/63) With our usual notation we write this as

$$\begin{aligned}\text{circumference} &= \sqrt{16a^2 + 24b^2} \\ &= 2a\sqrt{10}\sqrt{1 - \frac{3}{5}e^2},\end{aligned}$$

where e is the eccentricity of the ellipse, so that $b^2 = a^2(1 - e^2)$. The formula may also be written

$$2a\pi\sqrt{1 - \frac{3}{5}e^2},$$

for Mahāvīra takes $\sqrt{10}$ to be the value of π. The exact value is given by the elliptic integral

$$4a\int_0^{\pi/2}\sqrt{1 - e^2\sin^2 t}\,\mathrm{d}t$$

which can be looked up in tables for a range of values of e between 0 and 1. The comparison below, in which a is taken to be 1, indicates the remarkable degree of approximation attained by Mahāvīra's simple formula.

e^2	Integral	Mahāvīra
1/4	5.870	5.792
1/2	5.402	5.256
3/4	4.844	4.659

Mahāvīra also gives a rule for calculating the area of a bow-shaped figure:

'In the case of a bow-shaped field, the calculated measure (of the area) is obtained by adding together (the measure of) the arrow and (that of) the string and multiplying the sum by half (the measure) of the arrow', (GSS 7/43) i.e.

$$\text{Area } = \tfrac{1}{2}(s + h)h.$$

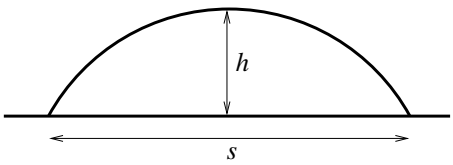


Figure 1.

One finds this formula in 'Nine Chapters on the Mathematical Art' (Chiu Chang Suan Shu), an ancient Chinese text of mathematics of about 200 BC. The Greek Heron (200 AD) gives the same rule and ascribes it to 'the ancients'. He knew that the rule is inaccurate. For a better approximation he quotes the formula

$$\frac{1}{2}(s + h)h + \frac{1}{14}\left(\frac{1}{2}s\right)^2.$$

According to Heron the above approximation is appropriate for segments in which $s < 3h$. For $s > 3h$, Heron gives another good approximation. It is surprising that Mahāvīra does not discuss these approximations, but the similarity suggests the possibility of a common origin. Mahāvīra, while giving an account of traditional geometrical knowledge, elegantly presents some original concepts also.

व्यासकृतिः षड्गुणिता द्विसंगुणायामकृतियुता (पदं) परिधिः

GSS 7/63.

कृत्वेषुगुणसमासं बाणार्धगुणं शरासने गणितम्

GSS 7/43.

In particular, his contribution to the generation of a right-angled triangle, whose diagonal is known, with the help of 'seed numbers' (which he calls bīja rāshi) is very important. He mentions three such rules; the third one is the most general and is as follows:

'Each of the various figures that are derived with the aid of the given seed numbers is written down; and by means (of the measure) of its diagonal the (measure of the) given diagonal is divided. The perpendicular side, the base and the diagonal (of this figure) as multiplied by the quotient (here) obtained gives rise to the perpendicular side, the base and the diagonal'. (GSS 7/122$\frac{1}{2}$)

If the seed numbers are $(m,\ n)$, then the following right-angled triangle is generated by them:

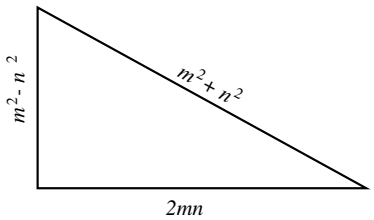


Figure 2.

$$\begin{aligned} \text{perpendicular} &= m^2 - n^2, \\ \text{base} &= 2mn, \\ \text{diagonal} &= m^2 + n^2. \end{aligned}$$

If the given diagonal is of measure c, then according to Mahāvīra the perpendicular, base and diagonal are respectively of measure

$$\frac{m^2 - n^2}{m^2 + n^2}\, c, \quad \frac{2mn}{m^2 + n2}\, c, \quad c.$$

Illustrating his rule he gives the measure of perpendicular and base for four such triangles whose diagonal is 65: $(25, 60, 65)$; $(33, 56, 65)$; $(16, 63, 65)$ and $(39, 52, 65)$ with the help of the seed numbers $(3, 2)$, $(7, 4)$, $(8, 1)$ and $(2, 1)$ respectively. For instance the pair $(3, 2)$ generates a right-angled triangle whose base is 12, perpendicular 5 and diagonal 13. If the required triangle has diagonal 65, then

$$\frac{c}{m^2 + n^2} = \frac{65}{13} = 5$$

So the three sides are $(60, 25, 65)$.

Using purely geometric techniques of ratios and proportions in similar figures, Mahāvīra in the ninth chapter of GSS gives rules and deals with problems concerning height and distances in trigonometry. The special features of these methods are their elegance and simplicity of presentation. The rule for calculating the shadow of a post due to a lamp is given as:

'The height of the lamp as diminished by the height of the post is divided by the height of the post. If, by means of the quotient so obtained, the (horizontal) distance between the lamp and the post is divided, the measure of the shadow of the post is arrived at'. (GSS 9/40$\frac{1}{2}$) Thus in the diagram,

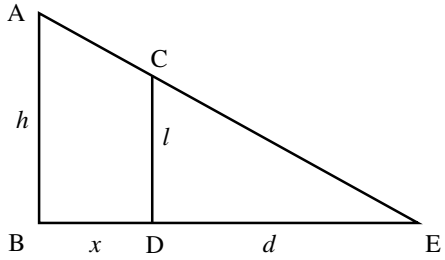


Figure 3.

AB $= h$, the height of the lamp;
CD $= l$, the height of the post;
BD $= x$, the distance between lamp and post;
DE $= d$, the shadow of the post.

Then, according to Mahāvīra,

$$d = x \div \frac{h - l}{l},$$

and this can be obtained from $\triangle$ABE and $\triangle$CDE:

$$\frac{AB}{CD} = \frac{BE}{DE} = \frac{BD + DE}{DE} = \frac{BD}{DE} + 1,$$

i.e.

$$\frac{AB - CD}{CD} = \frac{BD}{DE} \quad \text{or} \quad \frac{h - l}{l} = \frac{x}{d},$$

which is equivalent to (2).

यथक्षेत्रं जातं बीजैः संस्थाप्य तस्य कर्णेन
इष्टं कर्णं विभजेल्लाभगुणाः कोटिदो : कर्णः

GSS 7/122$\frac{1}{2}$

शंकुनिहतद्वीपोन्नतिराप्ता शंकुप्रमाणेन
तल्लब्धहृतं शंकोः प्रदीपशंकुन्तरं छाया

GSS 9/40$\frac{1}{2}$

इष्टादि द्विगुणेष्ट प्रचयेष्ट पदान्नयोऽनेष्ट कृतिः

GSS 2/44.

IV. Algebra

In algebra, apart from quadratic equations, Mahāvīra has significantly contributed to permutations and combinations and unit fractions. He is the first mathematician to have given the general formula for the number of ways of choosing r objects from n objects, which we write today as

$$^nC_r = \frac{n(n-1)(n-2)\cdots(n-r+1)}{1.2.3\ldots.r}.$$

One of his interesting ideas is in cubing, where he has given several methods based on progressions. One such method is described in GSS 2/44, that is, if the cube of an integer n is required, then let the first term be $a = n$, the common difference $d = 2n$ and the number of terms be n. Then the cube of n is the sum of this arithmetic progression. For we have the general formula

$$s_n = \tfrac{1}{2}n[2a + (n-1)d],$$

and taking $a = n$ and $d = 2n$ we obtain

$$\begin{aligned} s_n &= \tfrac{1}{2}n[2n + (n-1)2n] \\ &= \tfrac{1}{2}n[2n^2] \\ &= n^3. \end{aligned}$$

Thus we see that Mahāvīrācārya was an original mathematician of the highest calibre. He systematically organised the traditionally available mathematical knowledge and enriched it with his own contributions. The poetic presentation adds charm to his work. His place among Indian mathematicians is unique.

References

1. M. Rangacharya, *Ganita-Sāra-Sarigraha*, edited with English translation (Madras, 1912).
2. E. T. Bell, *Development of Mathematics* (New York, 1945).
3. L. C. Jain, *Ganita-Sāra-Sarigraha*, edited with Hindi translation (Sholapur, 1963).
4. C. N. Srinivasiengar, *The History of Ancient Indian Mathematics* (Calcutta, 1967).
5. A. L. Basham *The Wonder that was India* (New York, 1977).
6. B. L. van der Waerden, *Geometry and algebra in ancient civilisations* (Berlin, 1983).

Professor Mahesh Dube, *of the Mathematics Department in the Holkar Science College, Indore, India, specialises in the history of mathematics. He is keen to popularise mathematics, particularly among Hindi speakers. Other interests of his are poetry and music.*

Braintwister

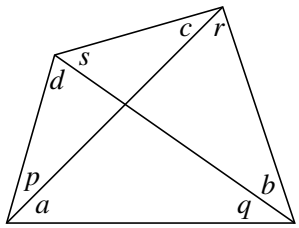
6. Square round robin

Seventeen players entered a 'round robin' squash tournament in which each player plays one game against each of the other players, and each game results in a win for one of the two players. At the end of the tournament each player counted up the total number of games he or she had won. Each of these totals turned out to be a positive perfect square.

What were the seventeen totals?

(The solution will be published next time.)

VICTOR BRYANT



Prove that

$$\sin a \sin b \sin c \sin d = \sin p \sin q \sin r \sin s.$$

P. TURVEY
(Brixton and Mayfair)

Prove that the sum to $2n + 1$ terms of the geometric series $x^n + x^{n-1} + x^{n-2} + \ldots$, where x is positive, is at least $2n + 1$.

Some Properties of the Number Five

J. D. WESTON

An intriguing exploration of the number Five.

The recurrence relation

$$n_{k+2} = 5n_{k+1} - n_k \quad (k = 0, 1, 2, \ldots), \tag{i}$$

together with the condition $n_0 = 1$, generates an infinite family of infinite sequences. Each member of this family is determined by its second term, n_1, subsequent terms being computable from (i) by iteration; and induction (on k) shows it to be a strictly increasing sequence of integers if n_1 is an integer greater than 1. We show that two of these sequences, namely

$$1, 2, 9, 43, 206, \ldots \tag{ii}$$

and

$$1, 3, 14, 67, 321, \ldots \tag{iii}$$

are related to each other in an interesting way.

The relation (i) is an example of a *homogeneous linear difference equation of the second order with constant coefficients.* (Another example is the well-known Fibonacci equation.) Such difference equations are encountered in various investigations, and their general theory resembles, but is simpler than, that of differential equations of the same description. (See, for example, the article 'Difference and Differential Equations' by G. N. Thwaites in *Mathematical Spectrum* **27** (1994/5), pp. 38–40.)

It is known — and easy to verify — that the difference equation

$$an_{k+2} + bn_{k+1} + cn_k = 0 \quad (a \neq 0)$$

is fully solved by the formula

$$n_k = Ap^k + Bq^k$$

when the quadratic equation

$$ax^2 + bx + c = 0$$

has unequal roots p and q, the constants A and B being determined from initial conditions, for instance prescribed values of n_0 and n_1. (The case of equal roots does not arise in the present discussion.) If, now, λ is one of the two (unequal) roots of the quadratic equation

$$x^2 = 5x - 1, \tag{iv}$$

the other root is λ^{-1} and the general solution of (i) is

$$n_k = \alpha\lambda^k + (n_0 - \alpha)\lambda^{-k} \quad (k = 0, 1, 2, ...), \tag{v}$$

where α is determined by the equation

$$(\lambda - \lambda^{-1})\alpha = n_1 - \lambda^{-1}n_0.$$

We take λ to be $\frac{1}{2}(5 + 21^{1/2})$, so that $\lambda^{-1} = \frac{1}{2}(5 - 21^{1/2})$. Then $\lambda - \lambda^{-1} = 21^{1/2}$ and therefore

$$21^{1/2}\alpha = n_1 - \lambda^{-1} = n_1 - \tfrac{1}{2}(5 - 21^{1/2}).$$

In case (ii), $n_1 = 2$ so that $21^{1/2}\alpha = -\frac{1}{2} + \frac{1}{2}21^{1/2}$, whence

$$\alpha = \tfrac{1}{2}(1 - 21^{-1/2}).$$

In case (iii), $n_1 = 3$ and it follows similarly that

$$\alpha = \tfrac{1}{2}(1 + 21^{-1/2}).$$

Thus if β denotes $\frac{1}{2}(1 - 21^{-1/2})$ then $\alpha = \beta$ in case (ii) and $\alpha = 1 - \beta$ in case (iii). Hence if μ denotes λ in case (ii) and λ^{-1} in case (iii) it follows from (v) that, in each case,

$$n_k = \beta\mu^k + (1 - \beta)\mu^{-k} \quad (k = 0, 1, 2, \ldots).$$

Also in each case, it follows from the quadratic equation (iv) satisfied by μ that

$$2\mu - 5 = 5 - 2\mu^{-1} \quad \text{and} \quad (2\mu - 5)^2 = 21,$$

and hence that, for $k = 0, 1, 2, \ldots$,

$$\begin{aligned} &2n_{k+1} - 5n_k \\ &\quad = 2(\beta\mu^{k+1} + (1 - \beta)\mu^{-k-1}) - 5(\beta\mu^k + (1 - \beta)\mu^{-k}) \\ &\quad = \beta(2\mu - 5)\mu^k - (1 - \beta)(5 - 2\mu^{-1})\mu^{-k} \\ &\quad = (2\mu - 5)(\beta\mu^k - (1 - \beta)\mu^{-k}), \end{aligned}$$

so that

$$\begin{aligned} (2n_{k+1} - 5n_k)^2 &= 21(\beta\mu^k - (1 - \beta)\mu^{-k})^2 \\ &= 21(\beta\mu^k + (1 - \beta)\mu^{-k})^2 - 84\beta(1 - \beta), \end{aligned}$$

and therefore, since $21\beta(1 - \beta) = 5$,

$$(2n_{k+1} - 5n_k)^2 = 21{n_k}^2 - 20. \tag{vi}$$

The sequences (ii) and (iii) thus consist of integers n having the property that $21n^2 - 20$ is the square of an integer. Suppose there are other positive integers with this property (at

least one other), and let n be the least of them. Then n is not 1 or 2 or 3 (since n is not in (ii) or in (iii)), so $n > 3$. Let

$$m := \tfrac{1}{2}(5n - (21n^2 - 20)^{1/2}).$$

Clearly $m > 0$, and $m < n$ since $21n^2 - 20 > 9n^2$. Also m is an integer; for if n is even the integer $(21n^2 - 20)^{1/2}$ is even, so $5n - (21n^2 - 20)^{1/2}$ is even, while if n is odd then $(21n^2 - 20)^{1/2}$ and $5n$ are odd, so $5n - (21n^2 - 20)^{1/2}$ is even. Moreover, $(2m - 5n)^2 = 21n^2 - 20$, so that

$$m^2 + n^2 = 5(mn - 1). \qquad \text{(vii)}$$

If $m = 1$ here then $n^2 - 5n + 6 = 0$; but n does not satisfy this equation, whose roots are 2 and 3. Hence $m > 1$ (so that $m \geqslant 2$); also,

$$\begin{aligned} 21m^2 - 20 &= 20(mn - 1) - 20mn + 21m^2 \\ &= 4(m^2 + n^2) - 20mn + 21m^2 = (2n - 5m)^2. \end{aligned}$$

From this it follows, since $1 < m < n$, that m is in (ii) or in (iii) and is n_k for some *positive* integer k. It follows also that

$$n = \tfrac{1}{2}(5m \pm (21m^2 - 20)^{1/2}).$$

Here the sign $\pm$ must be read as $+$; for, since $m > 1$, $21m^2 - 20 > 9m^2$ so the alternative reading would be inconsistent with the condition that $m < n$. Thus

$$n = \tfrac{1}{2}(5n_k + (21{n_k}^2 - 20)^{1/2}),$$

where $k > 0$. But (i) implies that if $k > 0$ then

$$2n_{k+1} - 5n_k = n_{k+1} - n_{k-1},$$

which is positive since (ii) and (iii) are strictly increasing sequences, and therefore, by (vi),

$$2n_{k+1} - 5n_k = (21{n_k}^2 - 20)^{1/2},$$

so that

$$n_{k+1} = \tfrac{1}{2}(5n_k + (21{n_k}^2 - 20)^{1/2}) = n,$$

contrary to the hypothesis that n is not in (ii) or in (iii). We have thus proved that

> ***the sequences*** (ii) ***and*** (iii) ***contain all and only those positive integers*** n ***for which*** $21n^2 - 20$ ***is the square of an integer.***

If $m = n_k$ and $n = n_{k+1}$, either in (ii) or in (iii), it follows from (vi), as in the derivation of (vii) above, that the equation (vii) holds. Conversely, let m and n be positive integers satisfying this equation: then $m \neq n$, since $3m^2 \neq 5$, and, as noted above,

$$21m^2 - 20 = (2n - 5m)^2,$$

so m is in one of the two sequences, say $m = n_k$. We assume that $n > m > 1$, and it follows as before that $n = n_{k+1}$, in the same sequence as m. Thus

> ***positive integers*** m ***and*** n ***satisfy the equation*** (vii) ***if and only if they are adjacent terms in*** (ii) ***or in*** (iii).

One might conjecture that the equation (vii) would have a solution in integers m and n if the coefficient 5 were replaced by some other positive integer. The following argument refutes this.

Let m, n, v be positive integers such that

$$m^2 + n^2 = v(mn - 1). \qquad \text{(viii)}$$

Then

$$(vm^2 - mn - 1)(mn - 1) = m^4 + 1. \qquad \text{(ix)}$$

The factors of $m^4 + 1$ are easily found when m is 1 or 2 or 3, and by equating these to $mn - 1$ in each case we find the values of n for which (ix) can then hold, and hence find that $v = 5$ in all those cases. Suppose then that, in (viii), $v \neq 5$ and m is minimal under this hypothesis. Thus $3 < m \leqslant n$.

From (viii) it follows that

$$v - 2 = ((m - n)^2 + 2)/(mn - 1), \qquad \text{(x)}$$

which is not an integer if $m = n$; thus $m \neq n$, so $m < n$. By the division algorithm, $n = qm + r$, where q and r are integers such that $q > 0$ and $0 \leqslant r < m$. We let $u := q + 1$ and $w := m - r$, so that $u \geqslant 2$, $0 < w \leqslant m$, and

$$n = um - w. \qquad \text{(xi)}$$

Substituting this expression for n in $vm^2 - mn - 1$, we see from (ix) that

$$(v - u)m^2 + wm - 1 = (m^4 + 1)/(mn - 1) > 0$$

and hence that $(v - u)m > -w \geqslant -m$, so $v - u > -1$, whence it follows that $u \leqslant v$ since u and v are integers.

If $u = 2$, then, by (x) and (xi),

$$v - 2 = ((m - w)^2 + 2)/(2m^2 - wm - 1),$$

which is not an integer if $w = m$; so $w < m$ in this case, so that $m^2 - mw > (m - w)^2$ and therefore

$$0 < v - 2 < ((m - w)^2 + 2)/((m - w)^2 + m^2 - 1) < 1,$$

a contradiction since v is an integer. Therefore $u \geqslant 3$. Now, by (viii) and (xi),

$$\begin{aligned} (u - v + 1)(mn - 1) &= (u + 1)(mn - 1) - m^2 - n^2 \\ &= (u + 1)(um^2 - wm - 1) - m^2 \\ &\qquad - (u^2m^2 - 2uwm + w^2) \\ &= uwm - u + um^2 - wm - 1 - m^2 - w^2 \\ &\geqslant uwm - u + um^2 - 3m^2 - 1 \\ &\geqslant uwm - u - 1 \geqslant 3(wm - 1) - 1 \\ &\geqslant 3(m - 1) - 1 > 0, \end{aligned}$$

so that $u - v + 1 > 0$, and therefore $u - v \geqslant 0$. Since, as we have seen, $u \leqslant v$, it follows that $u = v$. Therefore, by (ix),

$$um^2 - mn - 1 = (m^4 + 1)/(mn - 1),$$

so that, from (xi),

$$(wm - 1)(vm^2 - wm - 1) = m^4 + 1.$$

Hence $m^4 = (wvm - w^2 - v)m^2$, and therefore

$$w^2 + m^2 = v(wm - 1). \qquad \text{(xii)}$$

Now $w \neq m$ since $2m^2 = 2(m^2 - 1) + 2$ and this is not divisible by $m^2 - 1$; so $w < m$, and comparing (xii) with (viii) we see that m cannot be minimal as supposed. Thus

v ***can only be 5.***

J D Weston *is an Emeritus Professor of Mathematics in the University of Wales. He has four degrees from the University of London, the first and third in electrical engineering, the others in mathematics. After his 'conversion', which he underwent during several years as an engineer, his first university appointment was at Sheffield, whence he moved to Newcastle and then, after short periods at Pasadena and Berkeley, to Swansea as Head of the Department of Pure mathematics.*

The RSA Algorithm: A Public-Key Cryptosystem

MICHAEL J. WILLIAMS and LINDA J. S. ALLEN

RSA: A tough code to break.

1. Introduction

In 1975 a new era in cryptography began with the advent of public-key cryptography. In the standard private-key cryptography, for each pair of individuals that exchange secret messages, it is necessary that each pair know the coding and decoding schemes or keys. In addition, the key for coding can be reversed to obtain the key for decoding with approximately the same amount of computational effort as for coding. The number of secret keys required in private-key cryptography becomes a problem when a large number of people want to exchange secret messages; each pair must have knowledge of a set of keys (one for coding and one for decoding) that they keep secret from every other pair.

For example, if a group of 1000 people want to send messages using private-key cryptography, a total of $C_2^{1000} = 1000(999)/2 = 499,500$ different sets of keys are required and in a group of 100,000 people the number required is close to 5 billion. However, in public-key cryptography, the key for coding can be made public because decoding requires a prohibitive amount of computational effort, making it practically impossible to discover the decoding key. Thus, if a group of 1000 people want to send messages using public-key cryptography, 1000 public keys are required, one for each person, which are made available to the entire group in something equivalent to a telephone directory. Now, it is only required that each person keep their decoding key secret. In this manner, only 1000 coding and decoding keys are required as opposed to 499,500 in the private-key cryptosystem. Thus, it is easy to see that the security of private-key cryptosystems can be more easily compromised than public-key cryptosystems.

There are numerous private-key and public-key cryptosystems; three very good introductions to many of these cryptosystems are Beutelspacher [1], Deneen [4] and Sinkov [8]. The coding scheme in private-key cryptosystems generally uses modular arithmetic with a one-to-one transformation L that codes the message; its inverse transformation L^{-1} decodes the message. Therefore, if the transformation L is known, its inverse transformation L^{-1} can be determined. Also, the computations involved in calculating L^{-1} are comparable to those involved with L. In private-key cryptosystems, to keep the decoding scheme secret, the coding scheme must also be kept secret. On the other hand, public-key cryptosystems are distinguished from private-key cryptosystems in that it is computationally difficult to determine a decoding scheme directly from a public-key coding scheme.

In this article, a simple, powerful and well-known public-key cryptosystem, the RSA cryptosystem, is described. The history and the complete theoretical foundation of the RSA cryptosystem are summarized. This self-contained analysis demonstrates why and how the RSA cryptosystem works. In addition, it is shown that the RSA algorithm can be implemented easily on a computer algebra system such as Maple. A simple message is coded and decoded using Maple. The Maple programs are given in the Appendix.

2. The RSA cryptosystem

One of the simplest public-key cryptosystems and to date one of the most secure is the RSA cryptosystem. The initials RSA are taken from the last names of the three scientists who developed the system, Ron Rivest, Adi Shamir and Leonard Adleman [3]. The system is based on exponentiating the numerical message in a particular modulus that is very large. However, inverting the message or decoding it is not a simple task because it is necessary to find the prime factors of the modulus, currently a computationally time-intensive task if the number of digits is greater than 200. The computational complexity or number of operations (addition, subtraction, multiplication, division and comparison) needed to find the prime factors of a number with 200 digits is discussed in [9].

In 1977 the developers of the RSA cryptosystem presented a challenge to researchers to decode a message that was coded with the RSA system. The modulus was a number with 129 digits referred to as RSA-129. At the time the challenge was made, the time to decode the message was estimated as 40 quadrillion years [3]. However, in 1994, after 17 years of extensive efforts by researchers around the world, the prime factors of RSA-129 were calculated and the message deciphered: 'The magic words are squeamish ossifrage' ([2], [3]). The rapid advances in computer technology and in mathematical techniques that occurred during this period were not foreseen in 1977. Thus, for a secure RSA system more than 129 digits must be used for the modulus, and it has been suggested that the number of digits be 200 or greater [3]. Interesting historical accounts of the beginning of public-key cryptography and the problems related to RSA-129 can be found in references [2], [3] and [5]. A more in-depth description of the RSA cryptosystem than described here can be found in books by Beutelspacher [1] and Vanden Eynden [9].

The security of the RSA cryptosystem is based on keeping private two very large distinct prime numbers which will be denoted as p and q. The product of these primes is the modulus, $n = pq$. As we shall see, a coded message can be decoded if the two prime factors p and q are discovered. In addition to the modulus, to code a message, the exponent to which the numerical message is raised must be known; this exponent is denoted as e. The numbers n and e are public keys and are used to code a numerical message m, $m < n$, as follows:

$$c = m^e \bmod n, \tag{1}$$

where c is the residue or remainder when m^e is divided by n, i.e. $m^e = kn + c$ for k some non-negative integer and $0 \leqslant c < n$. Alternately, we say that m^e is congruent to c (mod n) and denote the expression (1) by $m^e \equiv c \mod n$. The message m may be a string of any number of letters (represented by two-digit numbers) provided that $m < n$.

Given the public keys e and n for coding, there is a private key d for decoding which is related to the public keys through the Euler phi function. The Euler phi function is defined for any positive integer n as the number of positive integers less than n that are relatively prime or coprime to n, and is denoted as $\phi(n)$ [9]. It will be shown that

$$\phi(n) = (p-1)(q-1) \tag{2}$$

for p and q prime and $p \neq q$. For example, if $n = 3 \times 7 = 21$, then $\phi(21) = 2 \times 6 = 12$. The integers less than $n = 21$ that are relatively prime to n are 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19 and 20, where the multiples of $p = 3$ and $q = 7$ are omitted; i.e. 3, 6, 9, 12, 15, 18, 7 and 14. In general, the $(q-1)$ factors of p and $(p-1)$ factors of q from 1 to $n-1$ are omitted, leaving

$$\begin{aligned} n - 1 - (q-1) - (p-1) &= pq - 1 - p + 1 - q + 1 \\ &= (p-1)(q-1) \end{aligned}$$

positive integers that are relatively prime to n. Thus, the formula (2) holds. Note that the formula is valid only if the primes are distinct, $p \neq q$, since $\phi(p^2) = p(p-1)$.

The private key d is related to the public key e and $\phi(n)$. The public key e is chosen to be a number relatively prime or coprime to $\phi(n)$, where $e > 1$. Then a private key d is chosen to be the multiplicative inverse of e modulo $\phi(n)$, i.e.

$$1 = ed \bmod \phi(n). \tag{3}$$

The private key is chosen to be the smallest positive solution to (3) so that $d < \phi(n)$. However, there is another smaller key that will decode the message also, that is, the solution of d

$$1 = ed \bmod \left[\frac{\phi(n)}{\gcd(p-1, q-1)} \right] = ed \bmod \psi(n), \tag{4}$$

where $\psi(n) = \phi(n)/[\gcd(p-1, q-1)]$ [1] and $\gcd(a, b)$ denotes the greatest common divisor of a and b. Irrespective of which of the two formulae is used to determine the private key d, calculation of d depends on knowledge of the prime factors p and q. Finally, the coded message c is decoded by raising c to the power d and finding its residue modulo n, i.e.

$$m' = c^d \bmod n. \tag{5}$$

It remains to be shown that the decoded message m' equals the original message m, i.e. $m = (m^e)^d \mod n$. In this case, the coding and decoding steps (1) and (5) define the RSA cryptosystem. Verification of the RSA cryptosystem follows from Fermat's Theorem which is stated below. First, a simple example of the RSA cryptosystem is given.

Suppose the message is the letter 'r', whose numerical equivalent is $m = 18$. Let the prime numbers be $p = 5$ and $q = 17$, so that $n = 85$ and $\phi(n) = 64$. Now, a public key e is chosen relatively prime to $\phi(n)$, say $e = 3$. The two public keys are n and e. The coded message for 'r' is

$$52 = (18)^3 \bmod 85.$$

The private key according to formula (3) is $d = 43$, since $1 = 3(43) \mod 64 = ed \mod \phi(n)$, or according to (4) is

$d = 11$, since $1 = 3(11) \bmod 16 = ed \bmod \psi(n)$. Applying the private key $d = 11$, decoding yields the original numerical message:

$$18 = (52)^{11} \bmod 85.$$

For large values of m, n and e the above procedures cannot be applied directly since m^e or c^d may have too many digits to be expressed computationally as an integer, which is a necessary prerequisite for the expression to be reduced modulo n. Thus, a practical method for coding is to first express e and d in binary form. For example, the binary representation of $d = 11$ is $d = 2^3 + 2^1 + 2^0 = 1011_2$. A more efficient method of evaluating $c^{11} \bmod n$ is

$$({c_3}^1 {c_2}^0 {c_1}^1 {c_0}^1) \bmod n,$$

where $c_0 = c$, $c_1 = c^2 \bmod n$, $c_2 = {c_1}^2 \bmod n$ and $c_3 = {c_2}^2 \bmod n$. In our example,

$$(52)^{11} \bmod 85 = (1)^1(1)^0(69)^1(52)^1 \bmod 85 = 18. \quad (6)$$

Another example is given in the last section.

Fermat's Theorem. *Let p be a prime number and let a be an integer such that p does not divide a. Then $1 = a^{p-1} \bmod p$.*

Proof. Consider the integers $1, 2, \ldots, p-1$, and multiply each by a to give $a \times 1, a \times 2, \ldots, a \times (p-1)$. No two of these can be congruent modulo p because, if $ra \equiv sa \bmod p$, then $r \equiv s \bmod p$ because a and p are coprime, so $r = s$ if they both lie between 1 and $p-1$. Moreover, $a \times 1, a \times 2, \ldots, a \times (p-1)$ cannot be congruent to 0 (mod p). Hence, $a \times 1, a \times 2, \ldots, a \times (p-1)$ are congruent to $1, 2, \ldots, p-1$ in some order, so that

$$1 \times 2 \times \cdots \times (p-1) \equiv (a \times 1)(a \times 2) \cdots (a \times (p-1)) \bmod p.$$

We can now cancel $1 \times 2 \times \cdots \times (p-1)$, which is coprime to p, to give $1 = a^{p-1} \bmod p$.

RSA Theorem. *If p and q are distinct prime numbers and m is an integer, then*

$$m = m^{ed} \bmod n.$$

Proof. By (3),

$$1 = ed \bmod (p-1)(q-1),$$

i.e. such that $ed = 1 + k(p-1)(q-1)$ for some positive integer k. The message m encodes to $m^e \bmod n$, which in turn decodes to $(m^e)^d \bmod n$. Thus, the RSA cryptosystem is verified by showing $m = m^{ed} \bmod n$. Verification depends on whether m is divisible by p or q.

Suppose m is divisible by p. Then

$$m \bmod p = m^{ed} \bmod p = 0.$$

If m is not divisible by p, then Fermat's Theorem applied to m and p gives

$$\begin{aligned} m^{ed} = m^{1+k(p-1)(q-1)} &= m \left[m^{(p-1)}\right]^{k(q-1)} \\ &\equiv m\, 1^{k(q-1)} \bmod p \\ &\equiv m \bmod p. \end{aligned}$$

In either case, it follows that $m^{ed} \equiv m \bmod p$. Similarly, $m^{ed} \equiv m \bmod q$. But, if a number is divisible by p and q, two distinct prime numbers, then it is also divisible by pq. Thus, $m^{ed} \equiv m \bmod pq$ or equivalently, $m = m^{ed} \bmod pq$.

In the proof we have used (3) to define the decoding key. A small modification is needed if (4) is used instead of (3). The proof is modified by replacing the definition of $ed = 1 + k(p-1)(q-1)$ by

$$ed = 1 + k(p-1)(q-1)/[\gcd(p-1, q-1)] = 1 + k\psi(n)$$

and noting that $\psi(n)$ is a multiple of $(p-1)(q-1)$.

3. Coding and decoding with Maple

The operations involved in the RSA cryptosystem can be carried out very simply using a computer algebra system. The computer algebra system Maple has many built-in functions that simplify calculations in modular arithmetic. For example, the public keys n and e can be selected such that $n = pq$ and $\gcd(e, \phi(n)) = 1$ with the help of the number theory package available in Maple. Given a positive integer p_1, the command nextprime(p_1) returns the smallest prime number greater than p_1 or prevprime(p_1) returns the largest prime number less than p_1. After two prime numbers, p and q, are generated, then $\phi(n)$ is known and a value for e can be chosen such that $\gcd(e, \phi(n)) = 1$. In our example,

$$n = 23235596443 \text{ and } e = 3817273,$$

where

$$p = 169567, \quad q = 137029, \quad \text{and } \phi(n) = 23235289848.$$

The following message 'the magic words are squeamish ossifrage' is coded using Maple. Each letter of the message is converted into a two-digit numerical equivalent; a space is denoted by 00 and the letters of the alphabet are denoted sequentially by the numbers 01 to 26. For lengthy messages the numerical message is divided into a sequence of blocks: $M_1, M_2, \ldots, M_l$ of fixed length, where $M_i < n$. In this example, the blocks are groups of five letters. Since the message 'the magic words are squeamish ossifrage' has a total of 39 letters and spaces, there are eight blocks $M_1, \ldots, M_8$ (a zero is added to the last block so that all blocks are the same length). The RSA algorithm

$$C_i = M_i^e \bmod n$$

yields the following eight coded blocks:

21560695345, 21602522120, 9312019215, 23005767162,
14025960459, 12733620991, 22058043497, 6247312421.

To implement exponentiation efficiently in modular arithmetic as in example (6), Maple uses the following symbolic operation & in addition to exponentiation: $M_i \& ^e \mod n$.

To decode this message, the secret key d is used; d has been calculated previously from the two primes, p and q and the public key e. Applying the function igcdex in Maple, an extended Euclidean algorithm, igcdex$(e, x, ' s', ' t')$, returns the greatest common divisor g of e and x such that $g = es + xt$. Thus, d is calculated from the formula (4) by letting

$$x = \psi(n) = \frac{\phi(n)}{\gcd(p-1, q-1)}\,.$$

It follows that the greatest common divisor of x and e is one, $1 = es + t\psi(n)$ or $1 - t\psi(n) = es$. The secret key $d = s \mod \psi(n)$. In our case,

$$d = 802794793.$$

(In the Maple programs in the appendix, the calculations to obtain the keys n, e and d are performed at the beginning of the first program.)

Decoding C_i with the RSA algorithm, $C_i \& ^d \mod n$ for $i = 1, \ldots, 8$ yields eight blocks which then must be converted to the original message. As one can see from the programs in the Appendix, much of the work in our Maple programs is devoted not to the RSA algorithm but to the conversion of the plaintext to its numerical equivalent or vice versa.

Unfortunately, our RSA algorithm in Maple is not secure. There are built-in functions in the number theory package that allow one to obtain the secret key d from n and e. The built-in function ifactor(n) returns the prime factorization of n and factorset(n) returns the prime factors of n. When either of these functions are applied to $n = 23235596443$ the prime factors $p = 169567$ and $q = 137029$ are obtained and the secret key can be found using the extended Euclidean algorithm function igcdex. For true security n should have more than 200 digits.

One final coded message is left as an exercise for the reader to decode. The public keys described in this example are applied to a message and coded as C_1, C_2, C_3, C_4, C_5, C_6, C_7:

$$9730034536,\ 18125299688,\ 18204717556,\ 10430426390,\ 4485284566,\ 16277148490,\ 10283958602.$$

Appendix
RSA Algorithm Implemented on Maple

Directions and Explanation:
Select three integers p1, p2 and p3 (between 6 and 10 digits in length). The two public keys n and e and the secret key d are generated from the three integers p1, p2 and p3 using the Maple package numtheory. (The keys n, e and d are denoted as nc, ec and dc, respectively, in the programs.) To code a message, type it below. The encryption program codes the plaintext message into a series of coded blocks using the public keys n and e. The decryption program decodes the coded blocks using the secret key d.

```
> p1:=169562: p2:=137001: p3:=3817270:
  with(numtheory):
  prime1:=nextprime(p1): prime2:= nextprime(p2):
  nc:=prime1*prime2;
  ec:=p3:
  cd:=2:
  while cd<>1
  do
   ec:=ec+1: cd:=gcd(ec,phi(nc)):
  od:
  ec:=ec;
  qc:=phi(nc)/gcd((prime1-1),(prime2-1)):
  igcdex(ec,qc,'dc','tc'):
  dc:=dc mod qc;
```

nc := 23235596443
ec := 3817273
dc := 802794793

Encryption

```
message:='the magic words are squeamish ossifrage';
n1:=5: size:=length(message);
```

message := the magic words are squeamish ossifrage
size := 39

```
> for x1 from 1 to size
  do
   ac(x1):=substring(message,x1..x1);
   for x2 from 1 to size
   do
   if ac(x2)=a then bc(x2):=1; elif ac(x2)=b then bc(x2):=2;
   elif ac(x2)=c then bc(x2):=3; elif ac(x2)=d then bc(x2):=4;
   elif ac(x2)=e then bc(x2):=5; elif ac(x2)=f then bc(x2):=6;
   elif ac(x2)=g then bc(x2):=7; elif ac(x2)=h then bc(x2):=8;
   elif ac(x2)=i then bc(x2):=9; elif ac(x2)=j then bc(x2):=10;
   elif ac(x2)=k then bc(x2):=11; elif ac(x2)=l then bc(x2):=12;
   elif ac(x2)=m then bc(x2):=13; elif ac(x2)=n then bc(x2):=14;
   elif ac(x2)=o then bc(x2):=15; elif ac(x2)=p then bc(x2):=16;
   elif ac(x2)=q then bc(x2):=17; elif ac(x2)=r then bc(x2):=18;
   elif ac(x2)=s then bc(x2):=19; elif ac(x2)=t then bc(x2):=20;
   elif ac(x2)=u then bc(x2):=21; elif ac(x2)=v then bc(x2):=22;
   elif ac(x2)=w then bc(x2):=23; elif ac(x2)=x then bc(x2):=24;
   elif ac(x2)=y then bc(x2):=25; elif ac(x2)=z then bc(x2):=26;
   else bc(x2):=0; fi:
   od:
  od:
  for x1 from 1 to n1-1
   do bc(size+x1):=0:
  od:
> for x1 from 1 to size by n1
  do
   bc1(x1+1):=bc(x1)*10 ∧ 2;
   for x2 from 1 to n1-2
   do
    bc1(x1+x2+1):=(bc1(x1+x2)+bc(x1+x2))*10∧2;
   od:
   block(x1):=bc1(x1+x2)+bc(x1+n1-1);
  od:
> for x1 from 1 to size by n1
  do
   code(x1):=(block(x1))&∧ec mod nc:
```

```
 od;
                        code(1) := 21560695345
                        code(6) := 21602522120
                       code(11) := 931201921
                       code(16) := 23005767162
                       code(21) := 14025960459
                       code(26) := 12733620991
                       code(31) := 22058043497
                       code(36) := 6247312421
```

Decryption

```
> for x1 from 1 to size by n1
    do
     decode(x1):=code(x1)&^dc mod nc:
    od;
                        decode(1) := 2008050013
                        decode(6) := 107090300
                       decode(11) := 2315180419
                       decode(16) := 1180500
                       decode(21) := 1917210501
                       decode(26) := 1309190800
                       decode(31) := 1519190906
                       decode(36) := 1801070500
> for x1 from 1 to size by n1
    do
     for x2 from 1 to n1
     do
      ad(x1+n1-x2):=decode(x1) mod 10^2;
      decode(x1):=(decode(x1)-ad(x1+n1-x2))/10^2;
     od;
    od;
> for x1 from 1 to size
    do
     if ad(x1)=1 then bd(x1):=a; elif ad(x1)=2 then bd(x1):=b;
     elif ad(x1)=3 then bd(x1):=c; elif ad(x1)=4 then bd(x1):=d;
     elif ad(x1)=5 then bd(x1):=e; elif ad(x1)=6 then bd(x1):=f;
     elif ad(x1)=7 then bd(x1):=g; elif ad(x1)=8 then bd(x1):=h;
     elif ad(x1)=9 then bd(x1):=i; elif ad(x1)=10 then bd(x1):=j;
     elif ad(x1)=11 then bd(x1):=k; elif ad(x1)=12 then bd(x1):=l;
     elif ad(x1)=13 then bd(x1):=m; elif ad(x1)=14 then bd(x1):=n;
     elif ad(x1)=15 then bd(x1):=o; elif ad(x1)=16 then bd(x1):=p;
     elif ad(x1)=17 then bd(x1):=q; elif ad(x1)=18 then bd(x1):=r;
     elif ad(x1)=19 then bd(x1):=s; elif ad(x1)=20 then bd(x1):=t;
     elif ad(x1)=21 then bd(x1):=u; elif ad(x1)=22 then bd(x1):=v;
     elif ad(x1)=23 then bd(x1):=w; elif ad(x1)=24 then bd(x1):=x;
     elif ad(x1)=25 then bd(x1):=y; elif ad(x1)=26 then bd(x1):=z;
     elif ad(x1)=0 then bd(x1):=' '; fi:
    od:
> message2:=bd(1):
    for x3 from 2 to size
    do
     message2:=cat(message2,bd(x3)):
    od: message2;
                the magic words are squeamish ossifrage
```


References

1. A. B. Beutelspacher, *Cryptology*, Spectrum Series (Mathematical Association of America, Washington DC, 1994).
2. J. Chan, Three guys and a large number, *Math Horizons* (February 1995), pp. 6–7.
3. B. Cipra, 'The magic words are squeamish ossifrage' *SIAM News* **27** (July 1994), pp. 12–13.
4. L. L. Deneen, Secret encryption with public keys, *The UMAP Journal* **8** (1987), pp. 9–29.
5. W. Diffie, The first ten years of public-key cryptography, *Proceedings of the IEEE* **76** (1988), pp. 560–577.
6. R. Honsberger, *Mathematical Gems*, The Dolciani Mathematical Exposition Series (Mathematical Association of America, Washington DC, 1973).
7. C. S. Ogilvy and J. T. Anderson, *Excursions in Number Theory* (Oxford University Press, New York, 1966).
8. A. Sinkov, *Elementary Cryptanalysis,* New Mathematical Library (Mathematical Association of America, Washington DC, 1966).
9. C. Vanden Eynden, *Elementary Number Theory,* Birkhäuser Mathematics Series (McGraw-Hill, New York, 1987)

Answer to coded message $C_1,\ C_2,\ C_3,\ C_4,\ C_5,\ C_6,\ C_7$ is 'mathematics is the key to success'.

Michael J. Williams *researched the RSA algorithm as part of his undergraduate research project in the Department of Mathematics at Texas Tech University. Currently, Michael is a graduate student at Texas Tech University pursuing a Master of Science degree in Statistics.*

Linda J. S. Allen*, an Assosiate Professor of Mathematics at Texas Tech University, served as the director of Michael's project. Her research interests include biomathematics and mathematical epidemiology.*

Royal Society Medals Awarded 1998: Copley Medal

Sir James Michael Lighthill FRS, has been posthumously awarded the Copley Medal in recognition of his profound contributions to many fields within fluid mechanics, including important aspects of the interaction of sound and fluid flow and numerous other contributions which have had practical applications in aircraft engine design. He is also noted for his groundbreaking work on both external bio-fluid-dynamics (analysis of mechanisms of swimming and flying) and internal bio-fluid-dynamics, including flow in the cardiovascular system and the airways, and cochlea mechanics and other aspects of hearing. Sir James' widow will collect the Medal on his behalf.

A Problem of Leonardo of Pisa

S. G. ROUT

This article explores an ancient and astonishingly fertile problem. It has a simple generalisation which continues to challenge mathematicians.

1. Introduction

The purpose of this article is to gather and develop some interesting strands surrounding what is commonly known as a problem of Leonardo (also known as Fibonacci). The question is to find a rational square which remains square when either increased or decreased by 5. This was in fact put to Leonardo about 1220, and had been investigated in a more general form (with some measure of success) by Arab mathematicians over two centuries earlier.

An Arab manuscript, written before the year 876, poses the problem of finding x(rational) such that, for a given integer k, the values of $x^2 \pm k$ are rational squares. (Thus Leonardo's problem is the special case where $k = 5$.) Knowledge of Pythagorean triples, and the identity

$$(x^2 + y^2) \pm 2xy = (x \pm y)^2$$

lead us to certain interesting special cases. For example, the 3,4,5 triangle leads to $5^2 \pm 24 = 7^2$ or 1^2. This provides a solution of the problem with $k = 24$, and division by 2^2 yields a solution of the problem with $k = 6$, namely, $(5/2)^2 \pm 6 = (7/2)^2$ or $(1/2)^2$. Generally, the above identity yields solutions when $k = 2xy$, where x and y are the shorter sides of a right-angled triangle, and k can be reduced by dividing out any square factors, as indicated. The Arab mathematicians managed to find solutions of their problem for $k = 5, 6, 14, 15, 21$ and higher values.

Leonardo solved the problem with $k = 5$, which was put to him by Johann Panormitanus of Palermo. In his 'Liber Quadratorum' of 1225 he asked how to find an integer which, when added to or subtracted from a rational square, gives rational squares. Or, in symbols, to find an integer k (called the *congruum)* and rational numbers a, b, c such that

$$b^2 - k = a^2 \text{ and } b^2 + k = c^2.$$

It seems natural to ask why the well-known case, namely that posed to Leonardo in 1220, concerns $k = 5$. Why 5? Why not a smaller integer? Surely this would sharpen the focus of the question? Well, no smaller integer allows a solution! In particular, taking $k = 1$, we would require the values of $(y/z)^2 \pm 1$ to be rational squares, and this implies solubility of the Diophantine equation $(y^2 + z^2)(y^2 - z^2) = t^2$, or $y^4 - z^4 = t^2$. This can be proved impossible by Fermat's method of infinite descent and, indeed, is essentially the same as Fermat's Last Theorem in the case of exponent 4. It is interesting that this apparently simple case was not conclusively settled until four centuries after Leonardo.

For what other values of k can x be found? $k = 6$ has the remarkably simple solution (also known to Leonardo) already mentioned here. The case $k = 7$ was solved by Euler, about 1770, with solution $x = 337/120$. In fact $(337/120)^2 + 7 = (463/120)^2$ and $(337/120)^2 - 7 = (113/120)^2$. This solution arises from the Pythagorean triple (175,288,337). For $(288^2 + 175^2) \pm 2 \times 288 \times 175 = (288 \pm 175)^2$, from which we get $337^2 \pm 7 \times 120^2 = 463^2$ or 113^2. Such values of k, for which a solution exists, are called *congruent numbers,* and they have found a connection with the theory of elliptic curves, which in turn were used in the final crackdown on Fermat's Last Theorem (by A. Wiles, in 1994).

2. Leonardo's problem solved

In this section I shall offer an elementary method of finding a solution of Leonardo's problem. In symbols, we seek rational x such that both values of $x^2 \pm 5$ are rational squares. Or, letting $x = y/z$, we need to find positive integers y, z such that both values of $y^2 \pm 5z^2$ are square numbers. In other words, $y^2 - 5z^2, y^2, y^2 + 5z^2$ form an arithmetical progression of squares.

We now make use of Pythagorean triples. It is well known that the integer sides of a right-angled triangle can be parametrized by

$$a = p^2 - q^2, \quad b = 2pq, \quad c = p^2 + q^2,$$

where p, q are integers, and a, b, c are assumed to have no common factor. But, if $a^2 + b^2 = c^2$, then

$$(a - b)^2, \quad c^2, \quad (a + b)^2$$

forms an arithmetical progression, with common difference $2ab$. We shall call this the 'associated progression' for the triple (a, b, c). Combining these observations, we get the progression

$$(p^2 - 2pq - q^2)^2, (p^2 + q^2)^2, (p^2 + 2pq - q^2)^2 \quad (1)$$

with common difference $4pq(p^2 - q^2)$.

We now seek p, q such that

$$4pq(p^2 - q^2) = 5z^2 \quad (2)$$

for some z. This possesses the easily observed solution $p = 5, q = 4$ (which leads to Leonardo's solution). But at this point we also observe that if p, q could be chosen to be sides of another right-angled triangle, with hypotenuse equal

to p, then $p^2 - q^2$ will be a square, which can be factored out, thus reducing the condition. It might be objected that this assumption seems to place restrictions on the set of *all* possible solutions, but this need not deter us in our search for *some* solution. Let us therefore suppose that (r, q, p) forms another Pythagorean triple, i.e. $q^2 + r^2 = p^2$, with $r = {p_1}^2 - {q_1}^2$, $q = 2p_1q_1$, $p = {p_1}^2 + {q_1}^2$. Condition (2) becomes

$$8({p_1}^2 + {q_1}^2)p_1q_1({p_1}^2 - {q_1}^2)^2 = 5z^2$$

or, more simply,

$$2({p_1}^2 + {q_1}^2)p_1q_1 = 5 \text{ (square number)} \qquad (3)$$

from which we see the immediate solution $p_1 = 2, q_1 = 1$. Substitution quickly leads to $a = 9, b = 40, c = 41$, a triplet with associated progression $31^2, 41^2, 49^2$ and common difference $5 \times 12^2 = 720$. Thus $41^2 \pm 5(12^2)$ are squares, and we have $x = 41/12$. This is Leonardo's solution.

3. Beyond Leonardo's solution

Are there other solutions? The benefits of Pythagorean triples continue to shower upon us as we now explore the possiblity that p_1, q_1 form part of yet another triple, with, say, $p_1 = {p_2}^2 - {q_2}^2, q_1 = 2p_2q_2$. Condition (3) now becomes

$$4({p_2}^2 + {q_2}^2)^2({p_2}^2 - {q_2}^2)p_2q_2 = 5 \text{ (square number)}$$

or, more simply,

$$({p_2}^2 - {q_2}^2)p_2q_2 = 5 \text{ (square number)},$$

which corresponds to (2), and from which we may use the previously observed solution $p_2 = 5, q_2 = 4$. Substitution now leads to some nice surprises:

$$p_1 = 9,\ q_1 = 40, \quad \text{whence} \quad p = 41^2,\ q = 720,$$

and progression (1) has common difference $= 4 \times 41^2 \times 720(41^4 - 720^2)$, from which $y = 41^4 + 720^2$ and $z^2 = 4 \times 41^2 \times 12^2(41^2 + 720)(41^2 - 720)$. Using our first solution in section 2, $z = 2 \times 41 \times 12 \times 31 \times 49$. Hence another solution to Leonardo's problem (in fact the next simplest!) is

$$x = (41^4 + 720^2)/(2 \times 41 \times 12 \times 31 \times 49)$$

or

$$x = 3344161/1494696.$$

The form of this second solution is highly suggestive: given one solution $x = y/z$, we look at the fraction

$$\frac{y^4 + 25z^4}{2yx\sqrt{|y^2 - 5z^2|(y^2 + 5z^2)}}.$$

We can set

$$y_1 = y^4 + 25z^4 \quad \text{and} \quad z_1 = 2yz\sqrt{|y^4 - 25z^4|}. \qquad (4)$$

That this does indeed provide us with a further solution is shown by the simplification

$${y_1}^2 \pm 5{z_1}^2 = (y^4 + 25z^4)^2 \pm 20y^2z^2(y^4 - 25z^4)$$

or

$${y_1}^2 \pm 5{z_1}^2 = (\pm y^4 + 10y^2z^2 \mp 25z^4)^2 \qquad (5)$$

and so ${y_1}^2 \pm 5{z_1}^2$ are both squares.

It is now possible to generate as many solutions as we wish, by repeated use of the transformation (4).

This method is readily generalized. If k is *any* congruent number, then there exist infinitely many values of x for which the values of $x^2 \pm k$ are the squares of rational numbers. For the algebraic relations (4) and (5) become

$$y_1 = y^4 + k^2z^4, \quad z_1 = 2yz\sqrt{|y^4 - k^2z^4|}$$

and

$${y_1}^2 \pm k{z_1}^2 = (\pm y^4 + 2ky^2z^2 \mp k^2z^4)^2.$$

Thus the simple solution $x = 5^2$ for $k = 6$ leads to $y = 1201$, $z = 140$ and the not so obvious solution $x = 1201/140$.

A particularly interesting observation at this point is the arithemetical progression $\mathrm{i}^2, 2^2, 3^2$,where $\mathrm{i} = \sqrt{-1}$. This has common difference 5, and provides the incredibly simple solution $y = 2, z = 1$, i.e. $x = 2$ (provided complex numbers are admissible). One wonders whether Leonardo looked at $2^2 \pm 5$ and ruefully resigned himself to the insolubility of $x^2 + 1 = 0$ (although perhaps this is expecting too much — in his day even negative numbers were treated with suspicion). It is even more ironic that application of (4) now yields $y_1 = 41$ and $z_1 = 12$, Leonardo's own solution.

4. A geometrical interpretation

The algebraic problem stated by the Arabs has a curiously simple geometric form, which was, not surpisingly, considered by the Greeks; that is, to find a right-angled triangle having rational sides and area equal to an integer. The simplest example is the 3,4,5 triangle, having area equal to 6, and this, as we have seen, is a congruent number. The case of area equal to 5 is a little trickier, the required triangle having sides of 3/2, 20/3 and 41/6.

The equivalence of the two versions of the problem results from the following considerations.

(a) If $p^2 + q^2 = r^2$ and $pq^2 = k$, then $(p \pm q)^2 = r^2 \pm 4k$ and so the values of $(r/2)^2 \pm k$ are rational squares.

(b) Conversely, if both values of $x^2 \pm k$ are rational squares, where k is an integer and x is rational, then the triangle shown has all sides rational and area equal to k.

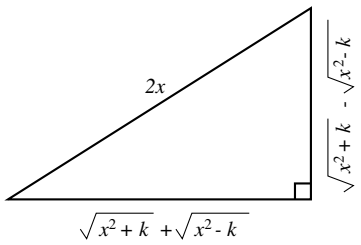


Figure 1.

5. A historical perspective

To this day it is an unsolved problem (indeed, perhaps the oldest unsolved problem in mathematics — see reference 3, appendix 6) to find a simple condition, both necessary and sufficient, to decide whether a given number is congruent (although it is an easy matter to find examples of congruent numbers). Clearly it is sufficient to consider only squarefree numbers: if k is congruent, then so is h^2k (where h is a positive integer), and conversely, as illustrated in the introduction to this article. It has been conjectured that a squarefree number is congruent if it is of the form $8n + 5$, $8n + 6$ or $8n + 7$, where n is a positive integer. As with Fermat's Last Theorem until recently, proof (or disproof) of this apparently straightforward statement seems elusive. The last word must go to Tunnell, and his remarkable theorem, which is deep, and difficult to prove (see reference 2).

Tunnell's Theorem. *Let n be an odd squarefree number. If n is congruent then the number of triples of integers (x, y, z) satisfying $2x^2 + y^2 + 8z^2 = n$ is equal to twice the number of triples satisfying $2x^2 + y^2 + 32z^2 = n$. Also, subject to a certain conjecture, the converse is true.*

It is a sobering thought that such an apparently straightforward problem as Leonardo's has such far-reaching consequences, and that its deepest secrets await discovery.

References

1. L. E. Dickson, *History of the Theory of Numbers*, Vol 2 (New York, Chelsea, 1966).
2. N. Koblitz, *Introduction to Elliptic Curves and Modular Forms* (Springer-Verlag, 1984).
3. Stuart Hollingdale, *Makers of Mathematics* (Penguin, 1989).

Stephen Rout *is Head of Mathematics at Queen Mary's Grammar School, Walsall. He attaches importance to encouraging students to ask searching questions, pose their own problems and seek alternative solutions, not necessarily in that order. He retains his sanity by playing the classical guitar.*

Solution to Braintwister 5
(The years in question)

Answer. 2032 and 2048

Solution:
Let Y be the year and let us try to express it as the sum of n consecutive integers, where $n > 1$ but n is as small as possible (and certainly less than Y). If n is odd the middle number in our sum will be Y/n and so we need that to be an integer. If n is even the middle two numbers of our sum will be

$$\tfrac{Y}{n} - \tfrac{1}{2} \quad \text{and} \quad \tfrac{Y}{n} + \tfrac{1}{2}.$$

So basically we need:

(a) n odd and Y/n an integer or

(b) n even and $2Y/n$ an odd integer.

For example, for $Y = 1998, n = 3$ works in (a) and $n = 4$ works in (b), and for $Y = 1999$ (and indeed for all odd Y), (b) works with $n = 2$. The first year with no such $n \leqslant 30$ is $2032 = 2^4 \times 127$; the lowest n which works in (b) is 127 and the lowest in (b) is 32.

Finding numbers which can never be expressed as a sum of consecutive positive integers requires a little more thought, but (a) and (b) imply that we need a number with no odd factors greater than 1; i.e. powers of 2. The next such year is $2048 = 2^{11}$.

VICTOR BRYANT

How much?

After every aspect of the running of the Copper Kettle Tearooms was taken over by a computer-controlled robotic system called CEDRIC, business boomed. This popularity, although not lessened by a tendency for CEDRIC's serving function to go into a loop, is based on two factors: firstly the unsurpassed quality of CEDRIC's home-baked scones; secondly, CEDRIC's small-talk, which becomes more suited to the customer as CEDRIC becomes better aquainted.

At the end of my last visit, I asked how much I owed for my biscuit and cup of coffee.

CEDRIC replied as follows:

- 8 coffees & 11 biscuits cost 5 pence more than 9 teas & 12 scones;
- 2 coffees & 5 biscuits cost 15 pence more than 2 teas & 5 scones;
- 3 coffees & 8 scones cost 5 pence more than 4 teas & 9 scones.

How much did I owe?

J. N. MACNEILL

Mathematics in the Classroom

Random Numbers

Ways of obtaining them

(i) Self-generated.

Many students confuse 'random' with 'haphazard' when it comes to obtaining a set of random numbers. This becomes apparent when they are asked to write down, without thought, one hundred single-digit numbers which they believe to be random. A chi-squared goodness-of-fit test usually exposes the selection as being *not* random in the statistical sense. So this method is not recommended.

(ii) Random number generators.

These are found on many computers and calculators but they also have their problems. These generators are able to produce observations from a continuous uniform distribution with range between 0 and 1, and truncated to 3 (say) decimal places, e.g. my calculator has just produced

0.871, 0.786, 0.040, 0.909, and 0.341

on pressing the appropriate button. But these are numbers which are generated by an algorithm and so are called *pseudo-random numbers*, although in practice, 'pseudo-' is usually dropped. Testing the randomness of these computer-generated numbers (which can also be reproduced in table form) is a popular coursework task commonly carried out, again using the chi-squared test. However, these pseudo-random numbers rarely fail to satisfy this check for randomness, so this is a recommended source.

What are they used for?

Random numbers are widely used in simulations and also in identifying members of a random sample selected with replacement. If it happens that the same sampling unit is selected twice, then an additional random number will identify a sampling unit as a replacement, ensuring that the sample is constituted of different units.

Recently a student observed that when using random numbers to identify a random sample of 50 students from a sampling frame of 500 students, then four students were selected twice, whilst none were selected more than twice. She felt that this was an unlikely event to have occurred. However, closer consideration reveals that an unlikely event would be the selection of n *different* units on the first attempt at achieving a 10% sample of size n, as long as n is large enough.

As calculators have not the capacity to work out ${}^{500}C_{50}$, we will consider smaller sampling frames but each with a sample size n which is 10% of the population size.
For example, if the sampling frame contains 20 names, then $n = 2$.

Total number of ways of selecting 2 from 20 (with replacement) = $20^2 = 400$.

Total number of ways of selecting 2 from 20 (without replacement) = ${}^{20}P_2 = 380$.

Therefore, the probability of no repeats = 380/400 = 0.95 and hence, the probability of a repeat = 1 - 0.95 = 0.05.

The reader is left to verify the following probabilities for varying population sizes:

Population size	Sample size	Probability of at least 1 repeat
30	3	0.098
40	4	0.143
50	5	0.186
60	6	0.227
70	7	0.226
100	10	0.372
200	20	0.626
300	30	0.777
380*	38	0.853

$*$ This is the largest number that I could persuade my calculator to cope with!

It can be seen that convergence to a certainty seems to be a certainty.

The original problem of finding the probability of 4 students being selected twice when a sample of 50 is taken from a population of 500 is left as an exercise for the reader, but I look forward to receiving your solutions to publish next time.

Lottery numbers

Lottery numbers are drawn *without* replacement and so are not strictly random in their selection. Even so there are ${}^{49}C_6$ = 13 983 816 different possible combinations at each draw. The outcomes that have occurred to date are readily available on the Internet (including information on which of three possible machines was used to make the draw) and provide much ever-changing data for coursework tasks. Questions frequently asked are:

- Are the numbers occurring uniformly?
- Is the frequency of occurrence of any particular number unlikely under the hypothesis of randomness? (The number 44 seemed to occur with a frequency that had some worried in the early months of the lottery draw.)
- Is each machine performing consistently?

The possibilities seem limitless!

Statisticians seem unable to resist the lure of the opportunities presented by this plethora of data and they are beginning to turn their attention to more complex questions. Recently, John Haigh (reference 1) responded to the challenge of finding the probability distribution of the number of jackpot winners in a given week. He suggested that this was dependent on the number of tickets sold, but if this number was five times ${}^{49}C_6$, then the following approximate distribution is obtained:

x: No. of winners	$p(x)$	x: No. of winners	$p(x)$
0	0.180	9	0.022
1	0.162	10	0.016
2	0.140	11	0.012
3	0.112	12	0.009
4	0.091	13	0.006
5	0.070	14	0.005
6	0.055	15	0.004
7	0.040	16	0.003
8	0.030	17	0.044

I can see that it will not be long before my students are testing this distribution against their Internet-acquired data and hence another coursework task is born.

Acknowledgement

I am indebted to Chris Hufton for drawing my attention to the almost infinite possibilities of random numbers.

Carol Nixon

References

1. John Haigh, Problem page, *RSS News* **24** (Nov. 1996).

Computer Column

Mersenne Primes

In 1644, the French monk Marin Mersenne (1588–1648) claimed that the number

$$M_n = 2^n - 1$$

is prime for

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

and composite for all other $n < 257$. Mersenne was not quite correct: M_{67} and M_{257} are *not* prime. Furthermore, he missed three: M_{61}, M_{89} and M_{107} *are* prime. But considering that Mersenne did not have access to a computer, his claim was remarkably accurate.

With the advent of computers, mathematicians soon started the search for new Mersenne primes. In 1952, for instance, Raphael Robinson found five Mersenne primes: the 13th through to the 17th. In 1963, Donald Gillies found three: the 21st through to the 23rd. Then began a race. Makers of supercomputers competed with each other for the honour of finding the largest prime, and this meant testing for Mersenne primes: throughout history the largest known prime has usually been a Mersenne prime. (There was also a practical aspect to all this: running programs to search for primes is a good way of testing a computer system.) For many years, it seemed that the only way to search for Mersenne primes was to use a Cray supercomputer or its equivalent. And yet in 1998 Roland Clarkson, a student, used a humble Pentium PC to become the world-record holder for the largest prime! He found the 37th Mersenne prime: a huge 909,526-digit number.

How is it possible to use a PC to outperform a Cray? The answer came in early 1996, when a computer programmer called George Woltmann began the *Great Internet Mersenne Prime Search* (GIMPS). Woltmann wrote a very efficient program, based on the well-known Lucas–Lehmer test, to check numbers for Mersenne primality. His program was designed to run on a PC as a background process: whenever the computer was switched on the program would run — as long as the owner was not doing something else. Woltmann then asked for volunteers to use this software to search for primes in certain specified ranges, with GIMPS coordinating the effort and maintaining an Internet database of the results. Over 4200 people volunteered.

Scott Kurowski, another programmer, later wrote some software that enabled Woltman's program to communicate directly with the database over the Internet, without the need for human intervention. The result is that over 4200 PCs are linked together in the search for Mersenne primes; they deliver more computing power in one day than a single PC can deliver in one year. Clarkson found his prime by running the Woltmann and Kurowski software in the background for 46 days. (It would have taken a week if his computer had been running full-time on the problem.) It is the third Mersenne prime found by the GIMPS collaboration.

The goal of GIMPS is to test every Mersenne number with an exponent less than 5,260,000 by the year 2000. So there is still time for you to join in the hunt. Maybe you could find the new record holder! You can get information, and download the free software, by pointing your browser to:

`http://www.mersenne.org/prime.htm`

Stephen Webb

For the record, the 37 known Mersenne primes have the following exponents:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107,
127, 521, 607, 1279, 2203, 2281, 3217, 4253,
4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497,
86243, 110503, 132049, 216091, 756839, 859433,
1257787, 1398269,
2976221, 3021377

Letters to the Editor

Dear Editor,

Catalan numbers and polygon division

Regarding the historical circumstances surrounding the discovery of the Catalan sequence

$$\{c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7, \ldots\} = \{1, 1, 2, 5, 14, 42, 132, 429, \ldots\}$$

in the context of geometry, I write to correct a piece of information given in the article on Catalan numbers by Vun and Belcher (Volume 30 (1997/8), pp. 3–5). The insert on page 3 wrongly reads that Johann von Segner was the first person to tackle successfully the enumeration of polygon decompositions into internal triangles by non-intersecting diagonals. It would seem, in fact, to be Leonhard Euler who initially considered this question, writing briefly of it in a letter (sent by him from Berlin in 1751) to contemporary mathematician Christian Goldbach wherein we find solutions for polygons of side number $3, \ldots, 10$, and so the early terms $c_1, \ldots, c_8$ of the Catalan sequence (c_0 has no physical interpretation here). It is clear that he had also identified the (ordinary) generating function for the integers. Von Segner's work, entitled 'Enumeratio modorum, quibus figurae planae rectilineae per diagonales diuiduntur in triangula', actually appeared a decade later in Volume 7 of the Russian journal *Novi Commentarii Academiae Scientiarum Imperialis Petropolitanae*. Not only this, but the paper contained a simple, and serious, arithmetic error on which Euler commented in a summary type article published simultaneously in the same volume.

It is mentioned too, in passing, that Jacques Binet also studied the topic, which in my opinion is a little misleading as a statement given in isolation. The well-known 1838 paper by Catalan—through which the numbers of the sequence have come to be associated with him by name—was just one of a series of articles written by various authors on mathematical aspects of polygon division and disseminated over the immediate years 1838–1843. In addition, N. Fuss had already published the first paper on a more difficult generalised version of the problem in 1795, preceded by another (albeit relatively obscure) article on triangular division by S. Kotelnikow in 1766.

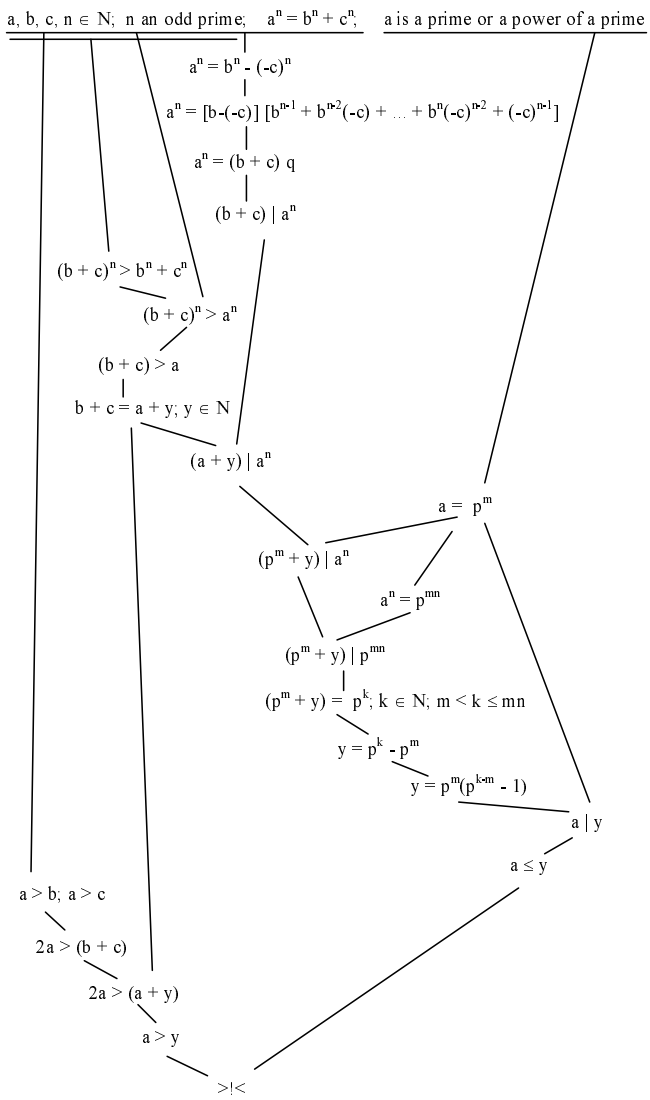
Yours sincerely,
PETER J. LARCOMBE
(School of Mathematics and Computing,
University of Derby, UK.)

Dear Editor,

Proof Maps

I have been thinking about ways of making the implicational structure of proofs more explicit and have developed a form of diagram which I call a 'proof map'. Readers may find it helpful to construct such a proof map for themselves when reading a mathematical argument.

As an illustration, in Volume 27 (1994/5), p. 12, John Sherrill gave a proof that the equation $a^n = b^n + c^n$ has no solution in natural numbers a, b, c and n when $n > 2$ and a is a prime or a power of a prime, a special case of Fermat's Last Theorem. Here is how the proof may be set out in a proof map:



The symbol $>!<$ denotes a contradiction.

Yours sincerely,
PETER DERLIEN
(School of Mathematics and Statistics,
University of Sheffield.)

Dear Editor,

Demonstrating divergence of series on a computer

In his letter (Volume 30, p. 44), Allen Brown offers a C program to give an indication of how slowly the harmonic series diverges. Since the precision of standard computer arithmetic is finite, great caution is needed in interpreting the results of such a program. Because of the continual rounding when terms are evaluated and summed, the sum to n terms as held by the computer is not in general accurate.

More strikingly, every *divergent* series with nth term tending to zero as n tends to infinity will appear to be *convergent* when investigated using finite-precision arithmetic. This is because eventually a stage will be reached after which every term will be too small to alter the value of the sum as held by the computer.

It is possible of course to write a program to tackle these difficulties; I found the sum to 1,000,000,000 terms of the harmonic series to be 21.300048150234794401. . ..

Yours sincerely,
MARIO VELUCCHI
(Department of Computer Science,
University of Pisa, Italy.)

Dear Editor,

Problems 28.4 and 28.5

These problems asked for all solutions in integers of the equations $2^n + n^2 = m^2$ and $3^n + n^3 = m^3$; the former has the only solution $n = 6, m = 10$ and the latter has no solution. In my Letter to the Editor in *Mathematical Spectrum* **30**, p. 42, I showed that the equation $2^x + x^2 = y^n$ has no solutions such that x is odd and $n > 1$. In this letter I prove the following.

Theorem. *The only solutions of the equation*

$$2^x + x^2 = y^n \tag{1}$$

such that $n > 1$ *are given by*

$$2^2 + 2^2 = 2^3$$
$$2^4 + 4^2 = 2^5,$$

and

$$2^6 + 6^2 = 10^2.$$

Proof. We may assume that n is prime. The case $n = 2$ is just Problem 28.4. Hence, we may assume that $n \geqslant 3$. Since the case x is odd was treated in my letter, it follows that we need only consider the case x is even.

Let $x = 2^m z$, where $m \geqslant 1$, and z is odd. Equation (1) can be rewritten as

$$2^{2^m z} + 2^{2m} z^2 = y^n,$$

or

$$2^{2m}(2^t + z^2) = y^n, \tag{2}$$

where $t = 2^m z - 2m$. Since

$$2^m \geqslant 2m, \tag{3}$$

and equality in (3) is obtained if and only if $m = 1$ or 2, it follows that

$$t = 2^m z - 2m \geqslant 0, \tag{4}$$

and equality in (4) is obtained if and only if $z = 1$ and $m = 1$ or 2. If $z = 1$ and $m = 1$ or 2, we obtain $x = 2$ or 4, which lead to the solutions

$$2^2 + 2^2 = 2^3$$

and

$$2^4 + 4^2 = 2^5.$$

From now on we assume that either $z \geqslant 3$ or $m \geqslant 3$. In this case, $t \geqslant 2$. Write $y = 2^\alpha u$, where $\alpha \geqslant 1$ and u is odd. Equation (2) becomes

$$2^{2m}(2^t + z^2) = 2^{\alpha n} u^n. \tag{5}$$

Since $t > 0$, it follows that $2^t + z^2$ is odd. Identifying the powers of 2 in equation (5) we get

$$2m = \alpha n$$

and

$$2^t + z^2 = u^n. \tag{6}$$

We investigate equation (6). Since $t = 2^m z - 2m$ is even one may rewrite equation (6) as

$$(z + \mathrm{i}2^{t/2})(z - \mathrm{i}2^{t/2}) = u^n.$$

Since $\mathbb{Z}[\mathrm{i}]$ is euclidean (i.e. it has unique factorization) and as

$$\gcd(z + \mathrm{i}2^{t/2}, z - \mathrm{i}2^{t/2}) = 1,$$

it follows that there exist $a, b \in \mathbb{Z}$ such that

$$z + \mathrm{i}2^{t/2} = (a + \mathrm{i}b)^n, \tag{7}$$

and

$$z - \mathrm{i}2^{t/2} = (a - \mathrm{i}b)^n. \tag{8}$$

In particular,

$$u = a^2 + b^2. \tag{9}$$

From (7), (8), the fact that n is odd and the binomial expansion, it follows that

$$z = \frac{(a+\mathrm{i}b)^n + (a-\mathrm{i}b)^n}{2} = al \tag{10}$$

for some integer l, and

$$2^{t/2} = \frac{(a+\mathrm{i}b)^n - (a-\mathrm{i}b)^n}{2i} = b(na^{n-1} + bs) \tag{11}$$

for some integer s. From equation (10) it follows that $a \mid z$. Hence a is odd. Since both u and a are odd it follows, by equation (9), that b is even. Since both n and a are odd and b is even, it follows that $na^{n-1} + bs$ is odd. From equation (11) it follows that $b = \pm 2^{t/2}$. Hence

$$u = a^2 + b^2 = a^2 + 2^t \geqslant 1 + 2^t.$$

From equation (6) it follows that

$$2^t + z^2 = u^n \geqslant u^3 \geqslant (1 + 2^t)^3 > 2^t + (2^t + 1)^2$$

so $z > 2^t + 1$. Then

$$t = 2^m z - 2m > 2^{t+m} + 2^m - 2m \geqslant 2^{t+m} \geqslant 2^{t+1} \tag{12}$$

with $t \geqslant 2$, which is not possible. Hence there are no further solutions.

Yours sincerely,
FLORIAN LUCA, Ph.D.
(Visiting Asst. Professor of Mathematics,
Syracuse University, New York.)

Problems and Solutions

Students are invited to submit solutions to some or all of the problems below. The most attractive solutions will be published in subsequent issues and are eligible for annual prizes. When writing to the Editorial Office, please state your full name and also the postal address of your school, college or university.

Problems

31.1 Prove that, for positive real numbers a, b, c,

$$\frac{abc\left(a+b+c+\sqrt{(a^2+b^2+c^2)}\right)}{(a^2+b^2+c^2)(ab+bc+ca)} \leqslant \frac{3+\sqrt{3}}{9}.$$

Can this be generalized?

(Submitted by Zhang Yun, The First Middle School of Jinchang City, Gan Su, China)

31.2 Are there three rational numbers whose product is 1 and whose sum is zero?

(Submitted by Peter Derlien, University of Sheffield)

31.3 (a) What are the probabilities of correctly picking exactly r numbers in the UK national lottery for values of r from 0 to 6?

(b) What is the probability that the winning numbers will have a common factor larger than 1? (The winning numbers are an unordered random choice of six distinct numbers from 1 to 49.)

31.4 Does the equation

$$x^4 = 2^n + 3^n + 5^n$$

have any solution for positive integers x, n?

(Submitted by Kenichiro Kashihara, Kanagawa, Japan)

Solutions to Problems in Volume 30 Number 2

30.5 Let a, b, c be positive real numbers. Prove that

$$(a+b+c)abc \geqslant 2a^2b^2 + 2b^2c^2 + 2c^2a^2 - a^4 - b^4 - c^4.$$

Solution by Jeremy Young, Nottingham High School.

We may suppose that $a \geqslant b \geqslant c$. Then

$$\begin{aligned}
&a^2(a-b)(a-c) + b^2(b-c)(b-a) + c^2(c-a)(c-b)\\
&\geqslant b^2(a-b)(b-c) + b^2(b-c)(b-a) + c^2(c-a)(c-b),\\
&= c^2(c-a)(c-b),\\
&\geqslant 0,
\end{aligned}$$

so

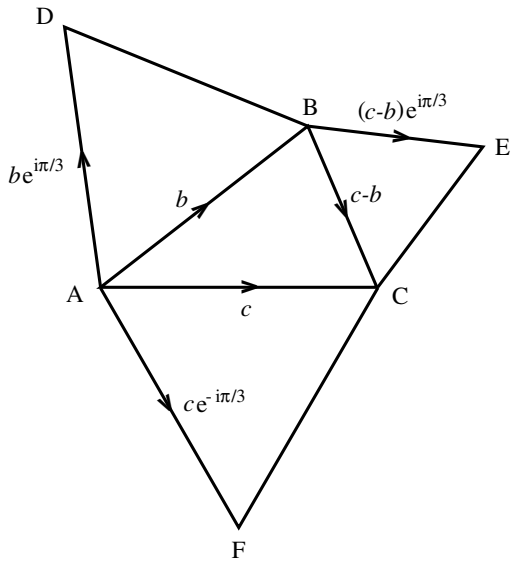
$$\begin{aligned}
a^4 + b^4 + c^4 + abc(a+b+c)&\\
&\geqslant a^3(b+c) + b^3(c+a) + c^3(a+b)\\
&= ab(a^2+b^2) + ac(a^2+c^2) + bc(b^2+c^2)\\
&\geqslant ab(2ab) + ac(2ac) + bc(2bc)
\end{aligned}$$

(since $a^2+b^2-2ab = (a-b)^2 \geqslant 0$). The result now follows.

Also solved by Ben Mulley (Gresham's School, Holt), Scott Brown (Auburn University, Alabama) and Ian Glover (Trinity Hall, Cambridge).

30.6 Given a triangle ABC, three equilateral triangles ABD, BCE and CAF are drawn external to the triangle ABC. Show that triangles ABC and DEF have the same centroid.

Solution by Tom Ross, Gresham's School, Holt



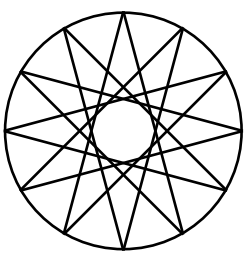
In the Argand diagram, with A as the origin, the centroid of $\triangle$ ABC is $\frac{1}{3}(b+c)$. The centroid of $\triangle$DEF is

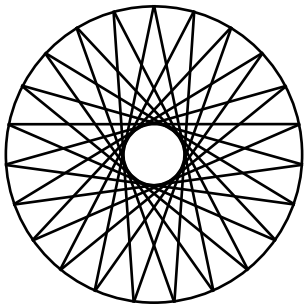
$$\begin{aligned}\tfrac{1}{3}\big(be^{i\pi/3} + b + (c-b)e^{i\pi/3} + ce^{-i\pi/3}\big) &= \tfrac{1}{3}\big(b + c(e^{i\pi/3} + e^{i\pi/3})\big)\\ &= \tfrac{1}{3}\big(b + 2c\cos\frac{\pi}{3}\big)\\ &= \tfrac{1}{3}(b+c),\end{aligned}$$

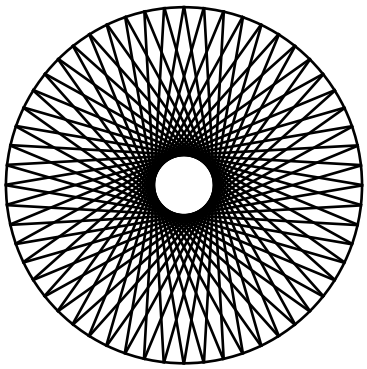
so the two centroids are equal.

Also solved by Mark Brimicombe (Christ Church College, Oxford) and Jeremy Young.

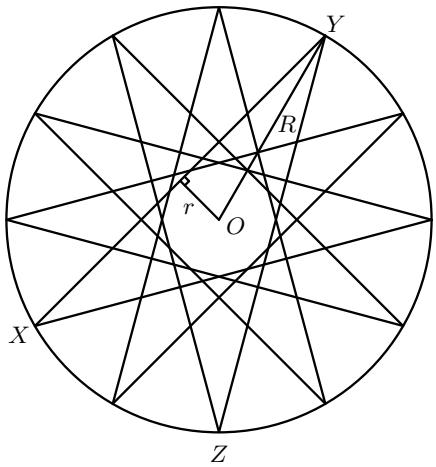
30.7 In the three diagrams shown, determine the ratios of the radii of the two circles.







Solution by Jeremy Young



Denote by n the number of vertices equally spaced round the large circle. Each vertex is joined to one m from it (say). (In the diagram, n=12 and m=5.) Then

$$\angle XOZ = \left(\frac{n-2m}{n}\times 360\right)^\circ,$$

$$\text{so}\quad \angle XYZ = \left(\frac{n-2m}{n}\times 180\right)^\circ,$$

$$\text{so}\quad \angle XYO = \left(\frac{n-2m}{n}\times 90\right)^\circ.$$

Thus

$$\frac{r}{R} = \sin\angle XYO = \sin\left(\frac{n-2m}{n}\times 90\right)^\circ,$$

The three cases given are:

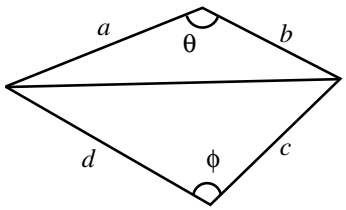
$$(m,n) = (5,12) \quad \text{giving } \frac{r}{R} = \sin 15^\circ,$$
$$(m,n) = (10,23) \quad \text{giving } \frac{r}{R} = \sin \frac{270^\circ}{23},$$
$$(m,n) = (25,56) \quad \text{giving } \frac{r}{R} = \sin \frac{135^\circ}{14},$$

so the respective ratios $R : r$ are approximately 3.86, 4.92, 5.97 (or nearly 4,5,6!).

Also solved by Kieran Gillick (Gresham's School, Holt).

30.8 Find the maximum area of a quadrilateral with sides of given lengths a, b, c, d in cyclic order.

Solution by Tim Raine, Gresham's School, Holt.



The area of the quadrilateral shown is

$$A = \tfrac{1}{2}ab\sin\theta + \tfrac{1}{2}cd\sin\phi,$$

with

$$a^2 + b^2 - 2ab\cos\theta = c^2 + d^2 - 2cd\cos\phi.$$

Thus

$$ab\sin\theta + cd\sin\phi = 2A,$$
$$ab\cos\theta - cd\cos\phi = \tfrac{1}{2}(a^2 + b^2 - c^2 - d^2).$$

If we square these equations and add, we obtain

$$a^2b^2 + c^2d^2 - 2abcd\cos(\theta+\phi) = 4A^2 + \tfrac{1}{4}(a^2 + b^2 - c^2 - d^2)^2$$

so

$$A^2 = \tfrac{1}{4}(a^2b^2 + c^2d^2) - \tfrac{1}{16}(a^2 + b^2 - c^2 - d^2)^2 - \tfrac{1}{2}abcd\cos(\theta+\phi).$$

The area is maximum when $cos(\theta+\phi) = -1$, i.e. $\theta+\phi = \pi$ (and the quadrilaterial is cyclic). The maximum area is

$$\left\{\tfrac{1}{4}(a^2b^2 + c^2d^2) - \tfrac{1}{16}(a^2 + b^2 - c^2 - d^2)^2 + \tfrac{1}{2}abcd\right\}^{\frac{1}{2}}$$
$$= \tfrac{1}{4}\left\{\left[(a+b)^2 - (c-d)^2\right]\left[(c+d)^2 - (a-b)^2\right]\right\}^{\frac{1}{2}}.$$

Also solved by Andrew Holland (Nottingham High School), Jeremy Young.

Reviews

Statistics. By ROGER FENTEM. Discovering Advance Mathematics Series, Collins Educational, London, 1996. Pp. x + 533. Paperback $11.99 (ISBN 0-00-322371-X).

This is an attractively laid out textbook designed to meet the needs of students of A- and AS-level syllabuses and the Common Core for mathematics. The text is visually pleasing with wide margins, tables and diagrams which are high-lighted by green shading, and the use of green type to identify section headings readily works well. The probability chapters also contain appealing pictures of dice, coins, balls in urns and other such stuff of which probability is made. The whole impression is one of a user-friendly, clearly presented text in language which is easy to read and, by inference, easy to understand.

Each chapter opens with bullet points listing its contents, and ends with a summary of the main points that have been introduced. In between, two sets of exercises follow each section of theory: set B mirroring set A so that the reader can practise the same work with different questions. Calculator activities are also suggested, where appropriate, although these might not always meet the needs of the average student as they tend to assume a full knowledge of all functions available to the calculator which is perhaps what the student is trying to achieve by working through the exercises! Each chapter concludes with consolidation exercises, many of which are problems taken from the examination papers of a variety of different exam boards.

There are no surprises in the content which is just what one expects from a book pitched at this level. Some ideas, though, are expressed more clearly than in the average textbook. Certainly the subtlety in difference between a box-and-whisper plot and a box-plot had previously eluded me. There is also a useful chapter on approaching coursework and, although it contains nothing new, students tend to be more influenced by advice in print than that emanating from their teacher.

On the minus side, the notation can be confusing. A section entitled *Does T+T+T always equal 3T?* and which concludes that the answer to this is No will only confound the problems that students have in distinguishing between sums of independent random variables and single variables multiplied by constants. Notation can also be cumbersome. The use of $P_{Av=3}(2)$ as a way of writing the probability that a Poisson random variable with mean 3 takes the value 2

is inelegant, and acknowledged to be so by the author who quickly drops it in favour of $P_3(2)$, which is not a big improvement. Careful proof-reading could perhaps have removed other confusions: the presence of a column entitled *Class width density* in a table demonstrating calculations for a histogram had me wondering if some new terminology had entered the subject. However, the presence of two columns, containing different numbers, but both headed *Frequency* give the clue to an experienced reader that the word *density* has strayed from its rightful column. Not an easy one for the student to unravel without help, and one shrinks in horror at the bad habits this might initiate.

The biggest problem with the book, however, is the absence of an index. Without such a listing, it becomes almost impossible for the student to use the book to locate a topic. Searching through the five pages of contents might not provide the whereabouts of the desired topic, and the inexperienced reader will have no idea of which chapter would be an appropriate place to scan.

This is not a text which I could happily leave with a student for self-study. As a trial I loaned it to a colleague who needed to teach himself some non-parametric tests. Despite his skills as a mathematician, he returned for a tutorial to sort out all the queries that the exposition had raised. Nonetheless, I can recommend it as a valuable source of examples and exercises and will certainly use it to support my own teaching.

Solihull Sixth Form College — CAROL NIXON

The Most Beautiful Mathematical Formulas. By LIONEL SALEM, FREDERIC TESTARD AND CORALIE SALEM. Wiley, UK, 1997. Pp. 156. Paperback $11.99 (ISBN 0-471-17662-1).

This is billed as an 'entertaining look at the most insightful, useful and quirky theorems of all time'. Excusing the formula/theorem mix-up, one might expect to find gems such as the Banach–Tarski paradox. Instead we find such illuminating results as 'The Area of a Rectangle is Equal to the Product of its Sides' and '$(a + b)(a - b) = a^2 - b^2$ '. To be fair, we do eventually get to more advanced material such as Goldbach's conjecture (surely neither a formula nor a theorem); these items are however, dealt with in a ridiculously brief fashion, as are others such as complex numbers.

The content is not helped by the appallingly patronising style which the authors adopt; results are introduced by means of narratives about cyclists and gardeners, all of which are irrelevant, space-consuming and in several cases highly misleading. To be fair, the authors devote a section at the back of the book to debunk their own myths; it might well have been best completely to omit them the first time. The most extraordinary manipulation of history occurs in the section on complex numbers, where 'Professor Sine' (another fictional character) tells how Euler humiliated Diderot by saying '$e^{i\pi} = -1$' so God must exist!'. In a foot-note, the authors explain that this did not happen, but instead give a quote from E. T. Bell's notoriously inaccurate 'Men of Mathematics' to provide the truth!

In summary, it is difficult to imagine who this book is aimed at; the style will be deeply patronising to anyone over the age of 8, and the vast majority of the content familiar to any A-level maths student. Not a book to be recommended.

Student, Trowbridge — TOBY GEE

Mathematical Analysis and Proof. By DAVID STIRLING. Albion Mathematics and its Application Series, Horwood Publishing Limited, Chicester. 1997. Pp. viii+244. Paperback $18.50 (ISBN 1-898563-36-5).

This book aims to introduce students to the idea of 'proof', and in particular to present well-motivated proofs of the elementary results of real analysis.

The early chapters show why proof is necessary and illustrate some of the common techniques, such as induction and contradiction. Naturally enough these chapters tend to be algebraic in nature and they give the reader plenty of practice in the manipulation of mathematical formulae.

Then the work proceeds to the more traditional material of a first analysis course, but with the proofs (and the reasons for them) explained very clearly. All this is interspersed with plenty of down-to-earth calculus examples. However the book also includes some quite technical results on power series and on integration and differentiation which in many institutions would be regarded as second year material.

For the most part this is a readable introduction to proof which gives a good overview of the approach to analysis, and therefore it would make a very suitable background reading book for a keen first or second year undergraduate. However it is hard to see how it would fit in as a main text book for any one course, partly because of the amount of material in it and partly because it cuts across the boundaries of the way in which algebra, analysis and proof are normally introduced.

University of Sheffield — VICTOR BRYANT

Other books received

Foundation Mathematics. By DR L. R. MUTOE AND DR M. BARRY. Wiley, Chichester, 1998. Pp. xii+656. Paperback $18.99 (ISBN 0-471-97092-1).

Mathematics in Engineering and Science. By DR L. R. MUTOE AND DR M. BARRY. Wiley, Chichester, 1998. Pp. xii+756. Paperback $18.99 (ISBN 0-471-97093-X).

These two large volumes take students on from UK GCSE level and include most of the mathematics needed to begin university courses in mathematics, engineering and the physical sciences.

Fundamental Ideas of Analysis. By M. REED. Wiley, UK, 1998. Pp. 413. Hardback $24.95 (ISBN 0-471-15996-4).

Calculus Volume 1. By H. ANTON Wiley, UK, 1998. Pp. 450. Paperback $17.99 (ISBN 0-471-24331-0).

Explorations in College Algebra. By L. A. KIME AND J. CLARK. Wiley, UK, 1998. Pp. 648. Paperback $35.50 (ISBN 0-471-10698-4).

Rings, Hopf Algebras and Brauer groups. Edited by S. CAENEPEEL AND A.VERSCHOREN. Marcel Dekker, USA, 1998. Pp. 332. Paperback $175.00 (ISBN-0-8247-0154-4).

Mathematical Spectrum

1998/9 Volume 31 Number 1

ISSN 0025-5653

Published by the Applied Probability Trust
Printed by Pear Tree Press Ltd, Stevenage, Herts, UK