Mathematical Spectrum

25TH YEAR OF PUBLICATION

1992/93

Volume 25

Number 2

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

Mathematical Spectrum 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.

Volume 25 of *Mathematical Spectrum* will consist of four issues, of which this is the second. The first was published in September 1992, and the third and fourth will appear in February and May 1993 respectively.

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 is also a section devoted to problems.

The Editorial Committee welcomes the submission of suitable material, including correspondence, queries and solutions to problems, for publication in *Mathematical Spectrum*. Students are encouraged to send in contributions. All correspondence about the contents should be sent to:

The Editor, Mathematical Spectrum,
Hicks Building, The University, Sheffield S3 7RH, UK

Mathematical Spectrum Awards for Volume 24

Prizes have been awarded to the following student readers for contributions published in Volume 24:

Jeremy Bygott;

Gregory Economides;

Nicholas Saltmarsh;

Amites Sarkar.

The Editors remind readers that prizes are available annually for student contributions as follows: up to the value of £50 for articles, and up to £25 for letters, solutions to problems, and other items.

Factorization: A Progress Report

PAUL LEYLAND, *University of Oxford*
JOSEPH McLEAN, *Strathclyde Regional Council*

Paul Leyland is a systems programmer at the University of Oxford Computing Services and, for the last few years, has been collecting and developing programs for the factorization of large integers and testing for primality. Joseph McLean works in the Finance Project Team of the Department of Information Technology of Strathclyde Regional Council in Glasgow, using a variety of computer equipment. He has developed many programs to deal with solutions of Diophantine equations, factorization and primality testing, and fractal geometry.

In an earlier article (*Mathematical Spectrum* Volume 21, pages 61–62), Joseph McLean referred to a factorization survey on numbers of the form $nx^n \pm 1$ which, for notational convenience, we shall later express as $n, x\pm$. The first part of the present article describes the current state of that survey and the methods used in reaching such an improved position. This is followed by an update report on the general state of factorization in the wider field.

Firstly, and to give some idea of the advances made, we can finally report that the tables for $2 \leqslant x \leqslant 9$ are complete for n up to 100. The results for $x > 4$ were obtained over a period of more than three years.

Most of the factoring was carried out by Paul Leyland on a variety of scientific workstations and using a number of methods which we shall describe later. Verifying primality is a crucial final step in factoring, and to perform this we initially required extensive subsidiary factorizations in order to use an implementation by Joseph McLean of Selfridge's improvement to the $p-1$ primality testing algorithm. Latterly, however, we obtained a version of the PARCL (Pomerance, Adleman, Rumely, Cohen and Lenstra) algorithm written for the UBASIC environment. UBASIC is a version of the BASIC programming language with support for multiple-precision arithmetic and a powerful set of number-theoretical functions. The interpreter was written by Yuji Kida and runs on IBM PCs and compatibles. The given program is able to test the primality of arbitrary 100-digit numbers in less than one hour.

After a number has been selected for factoring, the first step is to remove all very small prime factors by trial division. The next stage is to locate relatively small factors with Pollard's *rho* and $p-1$ methods and Williams' $p+1$ method. In this manner, primes smaller than 10 digits or so can be found, and occasionally much larger ones. If the unfactored residue is still composite (which can rapidly be determined by the Miller–Rabin algorithm), the heavy artillery is employed.

The heavy treatment consisted of a two-pronged attack: the elliptic curve method (ECM) and the multiple polynomial quadratic sieve method (MPQS). ECM is highly effective at locating factors of intermediate size passed over by lesser algorithms and occasionally achieves spectacular success with large factors. In the present survey, it almost always found all factors with fewer than 20 digits and sometimes found them with 30 or more. The running time of ECM is dependent primarily on the size of the smallest factor; it is only weakly dependent on the size of the number being factored. MPQS, on the other hand, has the opposite behaviour. The run time is independent of the factors but increases rapidly with the size of the number. The form of the algorithm, however, is such that it is relatively easy to share the workload between a number of machines working concurrently. A further benefit of MPQS is that it is guaranteed to find the factorization in a predictable time. Unfortunately, the run time is so long for numbers larger than 70 digits (with the resources available to us) that all other avenues had to be pursued first. Using an implementation written by Mark Manasse and Arjen Lenstra, Paul Leyland optimized the code to run on Sun workstations. Up to 50 workstations have been used for a single factorization, though a more typical run uses 8–12 machines.

A few examples of successful factorizations will illustrate the effectiveness of MPQS. For this we require the following definitions. A 'mips' (millions of instructions per second) is a measure of computing power, with the Digital VAX 11/780 minicomputer being the archetypal 1 mips machine. A 25-MHz 80386-based PC has a power of about 6 mips. A mipsday is a measure of power consumption and is equivalent to a VAX performing non-stop for one complete day of 24 hours. A mipsday is rather small for some of the work we have performed, and a mipsyear (defined in the obvious manner) is often more useful.

The large composite cofactor of 87, 9+ took just under one mipsyear to factor with MPQS—an elapsed time of 8.5 days on up to eight Sun-4's working simultaneously.

The cofactor of 97, 8− took 13.5 days to factor with MPQS, using up to 11 Suns and approximately 1 mipsyear.

The cofactor of 97, 9+ took a little over a week to factor, using a number of Sun-4's and a DEC DS3100—about 200 mipsdays.

The cofactor of 97, 9− was factored with a double-partial variant of MPQS running on a Sun SPARC-station II, a DEC DS5500 and a few, less-powerful, Sun workstations. The first two machines are rated at about 25 mips each. The whole process took precisely two months in real time and approximately one mipsdecade of processing power. At 91 digits, this is the largest successful factorization found by Paul Leyland within our survey.

The 92-digit composite cofactor of 99, 9+ was the last number in the survey to be factored. It would have presented major difficulties, requiring even more computing power than the mipsdecade just mentioned. However, Paul Leyland mentioned the problem to Arjen Lenstra, who promised to help. The successful factorization was duly delivered: it took less than 12 hours on a 16-k MasPar (a massively parallel processor machine, with 16384 independent CPUs).

The smallest Mersenne number remaining unfactored at the time of writing (February 1992) is $2^{467}-1$. The largest two successful factorizations using MPQS are of 113 digits (a cofactor of $10^{151}-1$) and 116 digits (a cofactor of $10^{142}+1$). These were both performed by Lenstra and Manasse and many others (including Paul Leyland) by splitting the various tasks involved between dozens of parties and collating the results. The largest successful factorization achieved anywhere is of the 148-digit cofactor of $2^{512}+1$, the 9th Fermat number, again by Lenstra, Manasse and many others. They used a new algorithm suggested by Hendrik Lenstra and now called the number field sieve (NFS). NFS is particularly powerful when applied to numbers of the form $x^n \pm d$ for small values of x and d. Excluding this special case, the current record holders for NFS are 124 digits (cofactor of $6^{163}-1$) and 125 digits (cofactor of $6^{164}+1$), both achieved by Bob Silverman. The composite cofactor of the 11th Fermat number has also been completely factored. Brent first located a factor with his own method and the residue was completed with MPQS by Alford and Pomerance.

Many factorizations of similar difficulty have been performed by Pomerance, Montgomery, Wagstaff and others, using highly optimized algorithms with processing shared between many scientific workstations. Very few factorizations are found by supercomputers these days, mainly due to their expense and rarity. Parallel processing is cheaper, easier to obtain and gives higher effective performance than a single supercomputer.

With the completion of the survey, Paul Leyland is now concentrating on the factorization of $n!\pm 1$ for $n \leqslant 100$, identifying primes of the form $n!\pm 1$, and the factorization of partition numbers in a competition being run by RSA Inc. He hopes also to turn his attention to the Cunningham project proper (which has as its aim the factorization of numbers of the form $x^n \pm 1$ for $x = 2, 3, 5, 6, 7, 10, 11$ and 12). Joseph McLean has currently extended the survey limit for $x = 2$ up to $n = 300$, and for $x = 3$ up to $n = 175$, though this part of the search has not yet been attacked with the heavier weaponry in the arsenal.

Bibliography

The first two books are general references. The first should be owned by every serious computer programmer (as should the other two volumes in the series). The second is an excellent introduction to the subject. It contains extensive tables and many computer programs, including a complete multiple-precision arithmetic package, and has a tutorial introduction to the number theory which underpins much of the subject. It is slightly dated in that it was published just before the ECM method was developed, but nonetheless should be consulted by everyone seriously attempting to factorize numbers or test them for primality. Both contain valuable historical material and extensive bibliographies.

1. D. E. Knuth, *The Art of Computer Programming—Volume 2 Seminumerical Algorithms*, second edition (Addison-Wesley, Reading, MA, 1981).

2. H. Riesel, *Prime Numbers and Computer Methods for Factorization* (Birkhäuser, Basel, 1985).

Modern factorization methods are well described in the following works.

3. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse and J. M. Pollard, 'The number field sieve', *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing*, Baltimore, 14–16 May 1990 ACM, 1990, 564–572.

4. A. K. Lenstra and M. S. Manasse, 'Factoring by electronic mail', *Lecture Notes in Computer Science* **434** (1990), 355–371.

5. H. W. Lenstra, Jr., 'Factoring integers with elliptic curves', *Annals of Mathematics* **126** (1987), 649–673.

6. P. L. Montgomery, 'Speeding the Pollard and elliptic curve methods of factorization', *Mathematics of Computation* **48** (1987), 243–264.

7. P. L. Montgomery, *An FFT Extension of the Elliptic Curve Method of Factorization*, PhD Thesis, UCLA, 1992.

8. R. D. Silverman, 'The multiple polynomial quadratic sieve' *Mathematics of Computation* **48** (1987), 329–339.

Nicolai Ivanovich Lobachevsky—The Copernicus of Geometry

ROGER WEBSTER, *University of Sheffield*

The author lectures in pure mathematics, his main interests being convexity and the history of mathematics. He is currently checking a book on convexity that he has written for Oxford University Press, and was promised for Easter 1973!

For over 2000 years Euclid's geometry as developed in his *Elements* (c. 300 BC) reigned unchallenged, both as a model of an axiomatic system and as a description of the world in which we live. This masterpiece of deductive reasoning quickly established itself as the definitive text on the subject and determined our conception of space right up until the 19th century. So completely did mathematicians accept Euclidean geometry that never once did they entertain the possibility of a completely different geometry capable of describing physical space. The first person to liberate geometry from its Euclidean stranglehold *and* publish an account of a non-Euclidean geometry was the Russian, Nicolai Ivanovich Lobachevsky. The English mathematician William Kingdon Clifford lecturing in 1873 waxed lyrical over Lobachevsky's achievement, likening it to that of Copernicus with his heliocentric theory of the universe, declaring: *What Copernicus was to Ptolemy, that was Lobachevsky to Euclid ... Copernicus and Lobachevsky each brought about a revolution in scientific ideas so great that it can only be compared with that wrought by the other.* To celebrate the bicentenary of Lobachevsky's birth, which falls in 1992, we tell the touching story of this founding father of non-Euclidean geometry.

Nicolai Ivanovich Lobachevsky, the second son of a minor government employee, was born on 2 December 1792 in Nizhni Novgorod (now Gorky) in Russia. The father died when Nicolai was only eight, leaving his widow to bring up their three young sons. She moved east with her family to remote Kazan, a picturesque city of some 25 000 inhabitants, where she enrolled the boys as free scholars at the local grammar school. Nicolai completed his studies brilliantly and in 1807, at the exceptionally young age of 14, entered the recently founded University of Kazan. Here he was to spend the rest of his life as student, professor, administrator and finally rector, a mathematical genius isolated on the intellectual periphery of Europe.

As an undergraduate Lobachevsky had the extreme good fortune to study under Martin Bartels, a former mathematics teacher of Gauss, and it was due to his influence that Lobachevsky developed a lifelong passion for mathematics. In 1811 he gained a master's degree for his *extraordinary successes and gifts in mathematical and physical sciences*, thus enabling him to pursue an academic career at the university. He was successively appointed assistant professor in 1814, associate professor in 1816 and full professor in 1822, excelling at research, teaching and administration. In 1820 he was made dean of his faculty, in 1822 he joined the committee formed to supervise the construction of new university buildings, in 1825 he became university librarian, and in 1827 he was elected rector, a post that he held for 19 years. The university prospered and grew as never before under his leadership; staff and student numbers increased, academic standards improved, scientific proceedings were published, and a complex of buildings, including a library, an astronomical observatory, science laboratories and a clinic, was constructed.

Lobachevsky's serious attitude to his duties made him appear withdrawn, perhaps even cold and aloof, but nothing could be further from the truth, for beneath the stern exterior beat a generous heart, as the many anecdotes about him bear witness. One story tells how he once observed a young clerk studying a mathematics book in his spare moments. With characteristic kindness, Lobachevsky helped the boy secure a place at the grammar school, from where he continued on to university, eventually succeeding to the chair of physics. Another story relates how the son of a poor priest, having trudged all the way from Siberia, arrived at Kazan in a much distressed state. Lobachevsky took the youth under his wing and set him off on a medical career. The favour was repaid with interest years later when the young man, having succeeded professionally, bequeathed a valuable library to the university.

Even after becoming rector, Lobachevsky did not consider it beneath his dignity to doff his coat and tackle the most menial task, should the circumstance warrant it. One day a distinguished foreigner, coming across the rector labouring in his shirtsleeves, mistook him for a caretaker and asked to be shown round the library. The visitor was so impressed by the courtesy and superior knowledge of his guide that he tendered a handsome tip, which Lobachevsky ungraciously declined. That evening, they were introduced to one another at the Governor's dinner table, where profuse apologies were offered and accepted on both sides.

Lobachevsky's love for his university was displayed no more vividly than during two natural disasters. When the virulent cholera epidemic sweeping across Europe reached Kazan in 1830, it was Lobachevsky's decisive action that prevented the university population from being decimated. He persuaded his colleagues to bring their families to the campus, where they were completely isolated, and stringent sanitary conditions were enforced. Of the 660 men, women and children thus protected,

Nicolai Ivanovich Lobachevsky 1792–1856

only 16 died—an almost negligible mortality rate compared with that of the town outside. When in 1842 a raging inferno destroyed half of Kazan, taking with it Lobachevsky's much prized observatory, he was quickly on the scene directing operations, and succeeded in saving not only the library, but also all the astronomical instruments from the flames. Without delay the indefatigable rector set about the task of rebuilding—in two years it was complete.

Praiseworthy though Lobachevsky's achievement in transforming Kazan University from an isolated cultural oasis into the model of a higher educational institution may be, it pales into insignificance compared to his discovery of non-Euclidean geometry; an event that has been described as the most consequential and revolutionary step in mathematics since Greek times. The Cantabrigian W. B. Frankland perhaps best captured the measure of Lobachevsky's mathematical achievement when he wrote in 1902:

> The task which Lobachevsky set himself was titanic. Throwing on one side the notorious parallel axiom, which ages failed to make

> clearer or surer, he rejected it for an unwarrantable assumption, and then audaciously faced the situation. The parallel axiom had not been proved; need it be true? With a prophetic instinct which is the hallmark of genius, Lobachevsky entirely discarded the incubus, and began to build up afresh the shrine of geometry so that it need not dread collapse if the parallel axiom were to fail. Theory and practice went hand in hand: he worked out on paper the theorems of a geometry in which the sum of the angles of a triangle was not two right angles, and he also searched the skies with his telescope to discover on that vast scale some sign of a measurable deviation.... In the teeth of an opposition sometimes bitter, and an indifference often contemptuous, he continued his researches, devoting himself whole-heartedly to the furtherance of truth. He was the apostle of unlearning, and therefore his lot was neither easy nor pleasant.

It is thus a dramatic tale that has to be told.

Our story begins over two millennia before Lobachevsky's birth with the most influential mathematics textbook ever written, Euclid's *Elements*. Euclid's aim in writing the *Elements* was to build the whole edifice of Greek geometrical knowledge on five carefully chosen *self-evident truths* called *axioms*. They were:

1. A straight line can be drawn from any point to any point.
2. A straight line can be produced continuously in a straight line.
3. A circle may be described with any centre and any radius.
4. All right angles are equal.
5. If a straight line falling on two straight lines makes the interior angles on the same side together less than two right angles, then the two straight lines, if produced indefinitely, meet on that side on which the angles are together less than two right angles. (See figure 1.)

From these few threads Euclid, the master craftsman, wove a rich and intricately designed tapestry to display his greatest treasures, results such as the angle sum of a triangle being two right angles and the celebrated Pythagorean theorem itself.

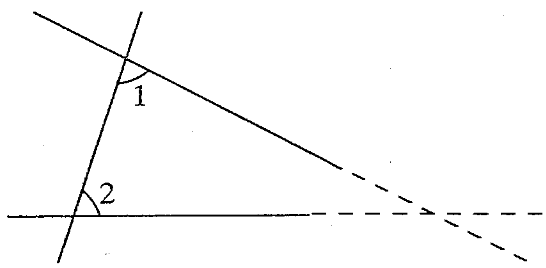


Figure 1. $\angle 1 + \angle 2 < 2$ right angles

The fifth axiom, usually referred to as the *parallel axiom*, has a sophistication that stands in stark contrast to the simplicity of the other four. Euclid's earliest commentators viewed it with scepticism, for reasons which are easy to find. Firstly, it was *not* self-evident. Secondly, it mentioned indefinitely producing a straight line and the Greeks mistrusted anything that might be construed as an infinite process. Euclid himself delayed using the axiom until he reached his 29th proposition, when he could not proceed without it. His development of geometry depends crucially upon the parallel axiom, as nearly all his results are established, either directly or indirectly, using it. To deny him access to it would be to deprive him of his greatest treasures.

One approach to the problem of the parallel axiom was to replace it with a more acceptable one. Of the many alternatives substituted for it over the years, the most popular has been the following: *Through a point not on a given line, there passes only one line which is parallel to the given line.* Recall that Euclid defines two lines to be *parallel* if they lie in the same plane and do not meet, however far they are extended. The above axiom, known as Playfair's axiom, is equivalent to the parallel axiom in the sense that, in the presence of the four uncontroversial axioms, they both give rise to Euclidean geometry. Thus Euclid's geometry can be considered as that developed from his first four axioms together with Playfair's axiom, and this we do.

A bolder attack on the problem was to try to deduce the parallel axiom from the other four, thus changing its status from axiom to theorem. The challenge to *prove the parallel axiom* attracted a distinguished line of mathematicians over the years, Greek, Arab and Western; many were convinced they had succeeded, their attempts only *later* being shown to be flawed. The confusion concerning the precise position occupied by the parallel axiom in the hierarchical structure of Euclid's geometry became something of a *cause célèbre*, with Sir Henry Savile, tutor to Elizabeth I, referring to it as a 'blot on geometry'. Unable to resolve the problem himself, he endowed the Savilian Chair of Geometry at Oxford University in the hope that one of its occupants would! This unsatisfactory state of affairs continued until the beginning of the 19th century when, in a case of simultaneous discovery never surpassed in the annals of mathematics, three men, working independently of each other, fathomed the 2000-year-old riddle of the parallel axiom. In so doing, they transformed not only man's conception of space, but also his views as to the nature of mathematics itself. The three revolutionary geometers were the German Carl Friedrich Gauss (1777–1855), the Hungarian Janos Bolyai (1802–1860) and the Russian Nicolai Ivanovich Lobachevsky (1792–1856), although the lion's share of the credit is usually given to the latter two, since Gauss did not have the moral courage to publish his findings on the subject.

Although Lobachevsky did research on algebra, analysis, mechanics and probability, it was the foundations of geometry that fired his imagination. Pedagogic considerations, arising out of teaching a geometry course, led to his initial interest in the parallel axiom. Like his predecessors he began by trying to prove it, but by 1825 he had become convinced that no proof was possible, writing:

> The fruitlessness of the attempts made since Euclid's time ... aroused in me the suspicion that the truth which it is desired to prove was not contained in the data itself.

Suspicion that the axiom could not be proved quickly grew into a conviction that there must exist a geometry in which it is violated. Thus Lobachevsky embarked on a journey of discovery that was to lead him to a strange new world in which Euclid's laws do not hold sway. With a missionary zeal, he set about constructing a non-Euclidean geometry, establishing its laws and deriving its trigonometry. He first made public his momentous discovery in a paper that he read to the mathematics faculty of Kazan University on 23 February 1826. No copy of the paper survives, but its ideas were incorporated into his *On the Principles of Geometry* published in instalments in the *Kazan Messenger* 1829–1830. This, the first account of non-Euclidean geometry to appear in print, marks the official birth of the subject.

Lobachevsky's wonderful creation, dubbed by him *imaginary geometry*, is founded on Euclid's first four axioms and the following one, in direct conflict with the parallel axiom: *Through a point not on a given line, there passes more than one coplanar line not meeting the given line.* The results that Lobachevsky discovered in his imaginary geometry were startlingly different from their analogues in Euclidean geometry, and would have frightened off less intrepid adventurers. To cite but a few examples: the angle sum of a triangle is *less* than two right angles; the area of a triangle is proportional to the amount by which its angle sum falls short of two right angles; similar triangles are congruent; and the circumference of a circle increases more rapidly than does its radius. Moreover, the points lying to one side of, and at a constant distance from, a given line do not lie on a line, but on a curve, thus causing a headache for Lobachevskian Railways!

Lobachevsky developed his geometry using trigonometrical formulae, abandoning classical geometric arguments in favour of function-theoretic ones. He observed that the trigonometric formulae, which he had so painstakingly established in his own imaginary geometry, could be readily found from the corresponding formulae of spherical geometry simply by replacing the sides a, b, c of the triangle by the purely imaginary numbers ia, ib, ic. Suppose, for example, that on the surface of a sphere of unit radius, a, b, c are the sides of a spherical triangle which has a right angle at the vertex opposite the side c. Then the spherical version of Pythagoras' theorem asserts that

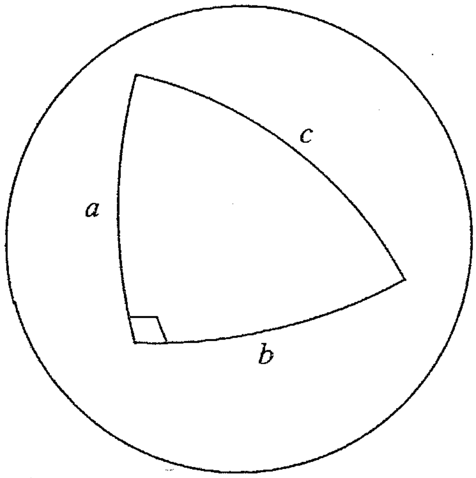


Figure 2. Spherical Pythagoras

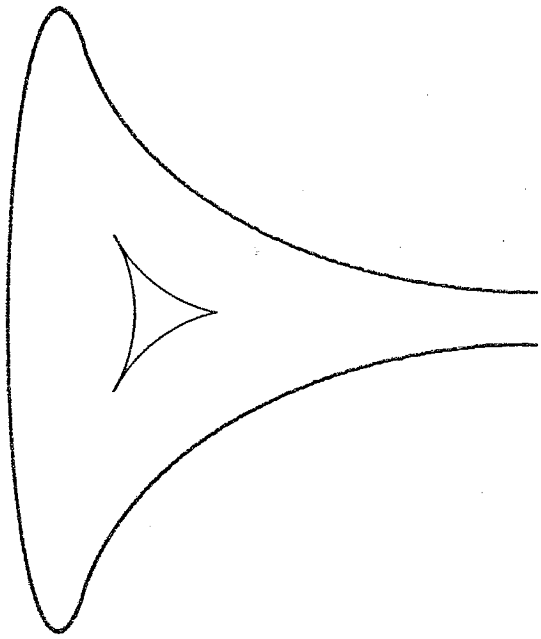


Figure 3. Triangle on a pseudosphere

$\cos c = \cos a \cos b$ (figure 2). Replacing a by ia, b by ib, c by ic and using the relation $\cos ix = \cosh x$, we find that $\cosh c = \cosh a \cosh b$, which is the version of Pythagoras' theorem appropriate to the Lobachevskian plane (when a certain constant attached to the plane is taken to be 1).

The deed was done, the news was out: geometries other than Euclid's *do* exist! The response, a resounding silence—the scientific world simply did not notice. No leading mathematician of the day offered a word of approval to the heretical geometer. Lobachevsky, aware of the significance of his discovery, strove to reach a wider European audience by publishing his *Theory of Parallels* (1840) in German, and his *Pangeometry* (1855) in French, but with only one definite success. Gauss learned of Lobachevsky's work from the German edition, and on his recommendation Lobachevsky was elected to the Göttingen Scientific Society in 1842, the only international recognition he received during his lifetime.

Why did Lobachevsky's non-Euclidean geometry fare so badly in terms of public response? True, he was unknown to the scientific community at large, but it was above all else the sheer daring of his enterprise that ensured a lukewarm reception. His ideas were too novel, too revolutionary, so that many years had to pass before they won general acceptance, which only came after his death. Two events were decisive in reversing the fortunes of the fledgling geometry. Firstly, Gauss's correspondence on the parallel axiom, published between 1860 and 1863, gave a great fillip to the cause when it revealed that the 'Prince of Mathematicians' had himself contemplated such a geometry. Secondly, in 1868 the Italian mathematician Eugenio Beltrami discovered the pseudosphere (figure 3), a surface resembling that of an infinitely drawn out horn, whose intrinsic geometry is Lobachevskian in the same way that spherical geometry is the natural geometry of the sphere. If the *line* through two points on the pseudosphere is taken to be the shortest path connecting them, then the resulting geometry of the surface is locally Lobachevskian. For example, it is easy to see that the angle sum of a triangle in this geometry is less than two right angles. By exhibiting this model of Lobachevsky's geometry on a Euclidean surface, Beltrami showed that the new geometry was as consistent as Euclid's own. This argument won the day in persuading the mathematical world to accept non-Euclidean geometry, and Lobachevsky and Bolyai were finally accorded the recognition they so justly deserved.

At a single stroke, the acceptance of non-Euclidean geometry not only resolved an ages-old problem—the parallel axiom was independent of Euclid's other assumptions, but also shattered the deep-rooted conviction that there was only *one* geometry. This had the far-reaching consequence of shifting the very foundations of mathematics itself. No longer could it lay claim to be a repository of truths inherent in the design of the universe, for it had been shown to be only a human creation, with the axioms of geometry being mere hypotheses, whose physical truth was of little concern! In the words of E. T. Bell in his book *Men of Mathematics*:

> In precisely the same way that a novelist invents characters, dialogues and situations of which he is both author and master, the mathematician devises at will the postulates upon which he bases his mathematical systems.

With this freeing of geometry from its traditional mould, the floodgates opened for the creation of a host of non-Euclidean geometries. In the classification process that ensued, the geometry of Lobachevsky and Bolyai also became known as *hyperbolic geometry*. Lobachevskian geometry continues to be researched on several fronts and has found applications to the description of space in Einstein's theories of relativity. This would have delighted Lobachevsky, who always saw his geometry grounded in measurement, even calculating the angle sums of celestial triangles to try to discover experimentally which geometry—his or Euclid's—actually occurs in the real world.

Not all Lobachevsky's energies were spent on professional duties, for family life and outdoor recreations also made a claim on his time. In 1832, at the age of 39, he married Varvora Moisieva, a well-to-do young lady with whom he had seven children. He purchased a smallholding at some distance from Kazan up the Volga, and here he would wile away the hours tending his gardens and orchards. The Lobachevskys enjoyed entertaining on their estate and during the vacations always included a group of disadvantaged students on their guest list. He took great pride in his prize flock of sheep and even discovered a new way of processing wool. All matters agricultural, horticultural and pastoral excited his lively interest.

The closing years of Lobachevsky's life were unhappy ones. The bitter disappointment he felt at failing to persuade the learned world to accept his ideas took its toll on his health, both physical and mental. In 1846, for reasons which are unclear, he was relieved of all his academic positions, causing him grave financial difficulties. Domestic tragedy struck when his eldest son died of tuberculosis at the age of 19. Even advancing blindness could not break Lobachevsky's spirit. His final book (on non-Euclidean geometry), published in 1855 as part of the University's 50th birthday celebrations, had to be dictated to a secretary.

A melancholy story tells how towards the end of his life he planted a grove of nut trees, but had a premonition that he would not live to taste their fruit. And indeed, on 24 February 1856, shortly after his foreboding, he died, and was buried in the newly-laid-out orchard. The trees bore their first fruit a few months later; the ideas that he had sown 30 years earlier took much longer to blossom.

Unusual Integration Formulae

P. GLAISTER, *University of Reading*

The author is currently a lecturer in mathematics at Reading University and has recently become interested in making the field of mathematics more widely understood by a population that is, on the whole, frightened of mathematics.

Using the identities

$$\sec^2 x = 1+\tan^2 x, \qquad \int \sec x \tan x \, dx = \sec x$$

and integration by parts, we have

$$\begin{aligned} I = \int \sec^3 x \, dx &= \int \sec x(1+\tan^2 x)\, dx \\ &= \int \sec x \, dx + \int (\sec x \tan x)\tan x \, dx \\ &= \ln(\sec x + \tan x) + \sec x \tan x - \int \sec^3 x \, dx, \end{aligned}$$

so that

$$I = \int \sec^3 x \, dx = \tfrac{1}{2}\{\ln(\sec x + \tan x) + \sec x \tan x\}.$$

We notice from this that

$$\int \sec^3 x \, dx = \tfrac{1}{2}\left(\int \sec x \, dx + \frac{d}{dx}\sec x\right),$$

i.e. $y = \sec x$ satisfies

$$\int y^3 \, dx = \tfrac{1}{2}\left(\int y \, dx + \frac{dy}{dx}\right), \tag{1}$$

an arithmetic mean. This is an unusual result and led to the investigation of other solutions $y = f(x)$ of (1).

By differentiation and rearrangement of (1) we have

$$\frac{d^2y}{dx^2} = 2y^3 - y,$$

and multiplying by dy/dx and integrating with respect to y we get

$$\left(\frac{dy}{dx}\right)^2 = y^4 - y^2 + A.$$

Integration of this results in

$$\pm \int \frac{1}{\sqrt{A + y^4 - y^2}} \, dy = x + B.$$

Choosing $A = 0$, $B = 0$ (and the positive sign) gives the solution found previously, i.e. $y = \sec x$, since

$$\int \frac{1}{\sqrt{y^4 - y^2}} \, dy = \int \frac{1}{y\sqrt{y^2 - 1}} \, dy = \sec^{-1} y.$$

Another solution is obtained by choosing $A = \frac{1}{4}$, $B = 0$ (and the positive sign). Since then

$$x = \int \frac{1}{\sqrt{y^4 - y^2 + \frac{1}{4}}} \, dy = \int \frac{1}{y^2 - \frac{1}{2}} \, dy = -\sqrt{2}\tanh^{-1}\sqrt{2}y,$$

$y = -\dfrac{1}{\sqrt{2}} \tanh \dfrac{x}{\sqrt{2}}$ also satisfies (1).

Readers are encouraged to investigate other solutions of (1) as well as looking for solutions of the natural generalisation of (1):

$$\int y^n \, dx = \tfrac{1}{2}\left(\int y \, dx + \frac{dy}{dx}\right) \quad (n \geqslant 2).$$

Angles in Platonic Solids

DERMOT ROAF, *Exeter College, Oxford*

The author was an undergraduate at Christ Church, Oxford and a graduate student in Cambridge. He is Mathematics Fellow at his college, with a particular interest in theoretical physics. His hobbies include bell-ringing (see *Mathematical Spectrum*, Volume 7, pages 60–66) and local politics: he is currently Leader of the Liberal Democrat Councillors on the Association of County Councils.

1. Introduction

Two recent problems (22.5 and 23.1) in *Mathematical Spectrum* asked for the angles subtended at the centre of a regular tetrahedron and of a regular icosahedron by an edge. The solutions printed (Volume 23, pages 27–28 and 96–98) did not use rotational symmetry, yet this gives interesting solutions. We will find the five angles (α to ϵ) subtended by an edge of each of the five platonic solids in turn, with the centre of each solid the origin and with unit lengths from each centre to each vertex.

The five platonic solids are regular, i.e. they have rotational symmetry in that every vertex can be rotated into the place of every other one. If the solid has exactly three edges meeting at a vertex, then there must be rotations of 120° and 240° about an axis through the origin and the vertex which leave the solid unaltered. If the axis were in the (1 1 1) direction, then the unit vector (1 0 0) would go to (0 1 0) and then to (0 0 1). Look at a cube along a body diagonal if you doubt this. As rotations are linear, an arbitrary vector

$$(p\ q\ r) = p(1\ 0\ 0) + q(0\ 1\ 0) + r(0\ 0\ 1)$$

would go (after 120°) to

$$p(0\ 1\ 0) + q(0\ 0\ 1) + r(1\ 0\ 0) = (r\ p\ q)$$

and to $(q\ r\ p)$ after 240°.

Similar rotations about the $(1\ -1\ 1)$ direction move $(1\ 0\ 0)$ to $(0\ 0\ 1)$ and then to $(0\ -1\ 0)$, so

$$(p\ q\ r) = p(1\ 0\ 0) - q(0\ -1\ 0) + r(0\ 0\ 1)$$

goes to

$$p(0\ 0\ 1) - q(1\ 0\ 0) + r(0\ -1\ 0) = (-q\ -r\ p)$$

and then to $(r\ -p\ -q)$.

2. The tetrahedron

A tetrahedron has only four vertices, each with three edges. If the unit vector from the centre O to the vertex A (see figure 1) is $(1\ 1\ 1)/\sqrt{3}$ and to another vertex B is $(p\ q\ r)$, the others, to C and D, are $(r\ p\ q)$ and $(q\ r\ p)$. The angle, α, between two unit vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ satisfies $\cos\alpha = \boldsymbol{a}\cdot\boldsymbol{b}$. So, for these vectors,

$$\frac{p+q+r}{\sqrt{3}} = \cos\alpha = pr+qp+rq.$$

Then

$$3\cos^2\alpha = (p+q+r)^2 = p^2+q^2+r^2+2pr+2pq+2qr = 1+2\cos\alpha.$$

This quadratic has roots $\cos\alpha = 1$ and $-\frac{1}{3}$. The first root corresponds to a single vertex, so the angle required is $\arccos(-\frac{1}{3}) = 109°28'16''$.

We have not had to find p, q and r and, indeed, there are infinitely many possible values. A symmetrical set is $p = 1/\sqrt{3}$, $q = -1/\sqrt{3}$ and $r = -1/\sqrt{3}$, so the complete set of vertices consists of $A\ (1\ 1\ 1)/\sqrt{3}$, $B\ (1\ -1\ -1)/\sqrt{3}$, $C\ (-1\ 1\ -1)/\sqrt{3}$ and $D\ (-1\ -1\ 1)/\sqrt{3}$.

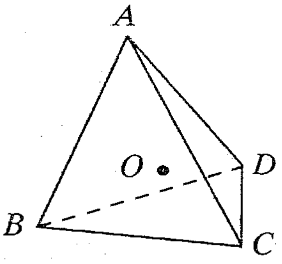


Figure 1. Tetrahedron

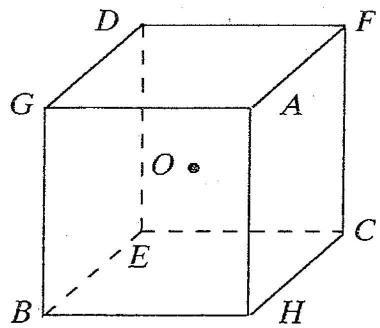


Figure 2. Cube

3. The cube

Similarly, three edges meet at each of the eight vertices of a cube. So the vertices (labelled A to H in figure 2) can be chosen (in that order) as $(1\ 1\ 1)/\sqrt{3}$, $(p\ q\ r)$, $(q\ r\ p)$, $(r\ p\ q)$, $(-1\ -1\ -1)/\sqrt{3}$, $(-p\ -q\ -r)$, $(-q\ -r\ -p)$ and $(-r\ -p\ -q)$, since the line from a vertex through the centre passes through the opposite vertex. The three vertices next to $H\ (-r\ -p\ -q)$ are $A\ (1\ 1\ 1)/\sqrt{3}$, $B\ (p\ q\ r)$ and $C\ (q\ r\ p)$. So

$$-\frac{p+q+r}{\sqrt{3}} = \cos\beta = -(pr+qp+rq),$$

giving

$$3\cos^2\beta = 1-2\cos\beta,$$

with roots 1 and $\frac{1}{3}$, so that the angle subtended by an edge is

$\arccos\frac{1}{3} = 70°31'44''$. Again a possible set of values is $p = 1/\sqrt{3}$ and $q = r = -1/\sqrt{3}$.

4. The octahedron

Four edges meet at each of the six vertices of an octahedron. But the faces are triangular. So we could rotate by 120° and 240° about a (1 1 1) axis through the centre of a face. The six vectors to the vertices (see figure 3) could be $X\,(p\ q\ r)$, $Y\,(q\ r\ p)$, $Z\,(r\ p\ q)$, $U\,(-p\ -q\ -r)$, $V\,(-q\ -r\ -p)$ and $W\,(-r\ -p\ -q)$. XZ and UZ subtend the same angle γ. So

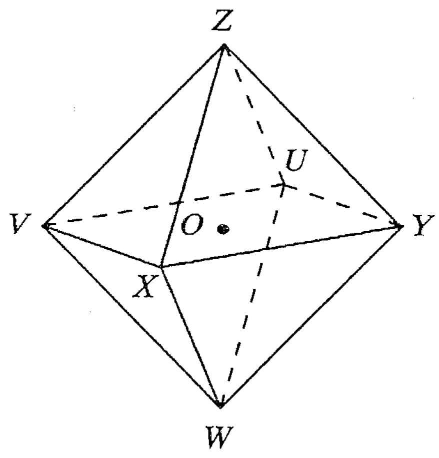


Figure 3. Octahedron

$$\cos\gamma = pr + qp + rq = -(pr + qp + rq).$$

Thus $\cos\gamma = 0$ and $\gamma = 90°$.

Alternatively we could rotate through 90°, 180° and 270° about a (1 0 0) axis through a vertex (X in figure 3) so that $Y\,(p\ q\ r)$ would go to $Z\,(p\ -r\ q)$, $V\,(p\ -q\ -r)$ and $W\,(p\ r\ -q)$. Then

$$(1\ 0\ 0)\cdot(p\ q\ r) = \cos\gamma = (p\ -r\ q)\cdot(p\ q\ r) \Rightarrow p = p^2,$$

so $p = 0$ or 1 and $\gamma = 90°$ or 0 ($\gamma = 0$ corresponding to a trivial single vertex). The simplest set of vectors is $X\,(1\ 0\ 0)$, $Y\,(0\ 1\ 0)$, $Z\,(0\ 0\ 1)$, $U\,(-1\ 0\ 0)$, $V\,(0\ -1\ 0)$ and $W\,(0\ 0\ -1)$. It may be noted that these vectors to the vertices of the octahedron pass through the midpoints of the faces of a cube, and vice versa.

5. The dodecahedron

The dodecahedron has 12 pentagonal faces and 20 vertices at which three edges meet. It can be seen in figure 4 that $AB = AC = AD = BC$, $AE = BF = CG = DH$ and $AF = FD = DG$ etc., so the tetrahedron $ABCD$ is regular and $ABCDEFGH$ is a cube. If we label the eight vertices A to H as in section 3 and if $I\,(p\ q\ r)$ is the vertex between $A\,(1\ 1\ 1)/\sqrt{3}$ and $H\,(1\ 1\ -1)/\sqrt{3}$, then, as $AI = IH$

$$\cos\delta = \frac{p+q+r}{\sqrt{3}} = \frac{p+q-r}{\sqrt{3}}.$$

So $r = 0$.

Rotations of 120° and 240° about OA (in the (1 1 1) direction) move $I\,(p\ q\ 0)$ to $J\,(0\ p\ q)$ and $K\,(q\ 0\ p)$. The angle subtended by IJ is the same as that subtended by AH ($\beta = \arccos\frac{1}{3}$), so

$$\tfrac{1}{3} = (p\ q\ 0)\cdot(0\ p\ q) = pq.$$

But

$$\cos\delta = \frac{p+q}{\sqrt{3}},$$

so

$$3\cos^2\delta = p^2+2pq+q^2 = \tfrac{5}{3}$$

and so

$$\delta = \arccos\tfrac{1}{3}\sqrt{5} = \arcsin\tfrac{2}{3} = 41^\circ 48' 37''.$$

We do not need to find the 12 non-cube vertices, but they can be shown to be $(\pm p\ \pm q\ 0)$, $(0\ \pm p\ \pm q)$ and $(\pm q\ 0\ \pm p)$. As $(p\ q\ 0)$ is a unit vector we can write $p = \cos\theta$ and $q = \sin\theta$. So

$$\sin 2\theta = 2pq = \tfrac{2}{3} = \sin\delta$$

and $\theta = \frac{1}{2}\delta$.

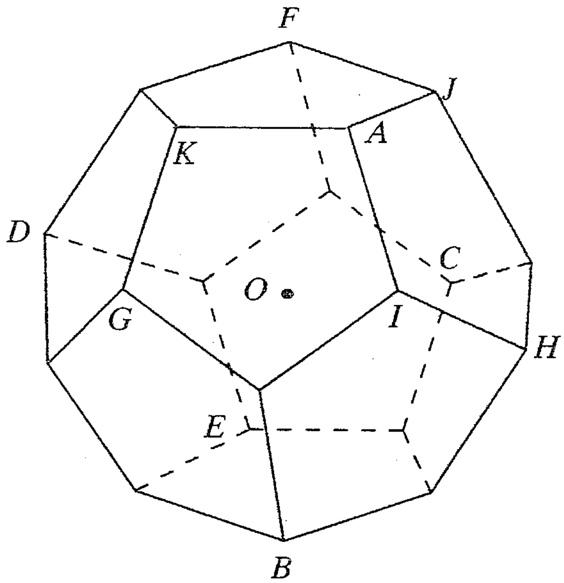


Figure 4. Dodecahedron

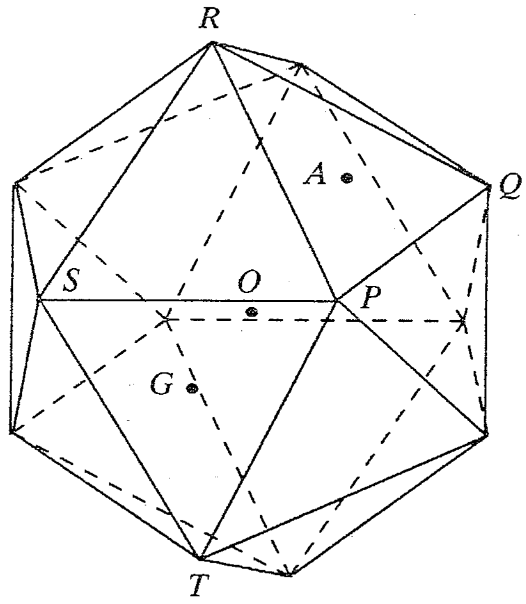


Figure 5. Icosahedron

6. The icosahedron

The icosahedron has five edges meeting at each of 12 vertices, but has 20 triangular faces. The centres of the faces are the vertices of a dodecahedron, just as the centres of the faces of a dodecahedron are the vertices of an icosahedron. So the centres of eight of the faces form a cube. Labelling these (see figure 5) as we did for the cube (A the midpoint of $\triangle PQR$ and G the midpoint of $\triangle PST$) and labelling the vertex P nearest to the line AG as $(p\ q\ r)$, we see that $q = 0$ (since $AP = PG$). Rotations of 120° and 240° about OA (the (1 1 1) direction) move P $(p\ 0\ r)$ to Q $(r\ p\ 0)$ and to R $(0\ r\ p)$. Rotations of 120° and 240° about OG (the $(1\ {-1}\ 1)$ direction) move P $(p\ 0\ r)$ to S $(0\ {-r}\ p)$ and then to T $(r\ {-p}\ 0)$ (see section 1).

PS and SR subtend the angle ϵ, so

$$rp = \cos\epsilon = -r^2+p^2.$$

If $p = \cos\phi$ and $r = \sin\phi$, this gives

$$\tfrac{1}{2}\sin 2\phi = \cos\epsilon = \cos 2\phi$$

or $\tan 2\phi = 2$, so

$$\epsilon = 2\phi = \arctan 2 = \arccos\frac{1}{\sqrt{5}} = 63°26'5''.$$

Again we do not need to find the vertices, but they can be shown to be $(\pm p\ 0\ \pm r)$, $(\pm r\ \pm p\ 0)$ and $(0\ \pm r\ \pm p)$.

7. Conclusion and further problems

There are no more platonic solids—if there were, I would set the problem of finding yet more angles subtended by an edge, to be done using the symmetry of rotations. As it is, I will have to ask you to calculate the angles subtended at the centre by non-adjacent vertices for these solids. (See the problem on page 58.)

Circular Motion in the Gas Laws: An Alternative Approach to Circular Motion

MARK FRENCH, *Longcroft School*

Mark French did his A-levels at Longcroft School, Beverley, Humberside. He is currently reading for a mathematics degree at St John's College, Oxford.

The ideal gas law $PV = \frac{1}{3}Mc^2$ is usually derived as follows. Consider a particle of mass m bouncing from side to side in a cubical box of width x at a constant speed $\dot{x}$ parallel to the side of the box. When the particle hits the wall of the box there is a momentum change of $2m\dot{x}$. Given that the time between collisions at the same wall is $2x/\dot{x}$, the average force on the wall is

$$\bar{F} = \frac{2m\dot{x}}{2x/\dot{x}} = \frac{m\dot{x}^2}{x}. \qquad (1)$$

The derivation proceeds as follows. The pressure on the wall (area x^2) is given by

$$\bar{P} = \frac{\bar{F}}{x^2} = \frac{m\dot{x}^2}{x^3} = \frac{m\dot{x}^2}{V},$$

where V is the volume x^3.

Now consider n particles, moving with a root mean square speed c. The mean value of $\dot{x}^2$ is $\frac{1}{3}c^2$, because a particle can move in any direction. Hence

$$P = \frac{mn \cdot \frac{1}{3}c^2}{V} = \frac{M}{3V}c^2.$$

Thus

$$PV = \tfrac{1}{3}Mc^2,$$

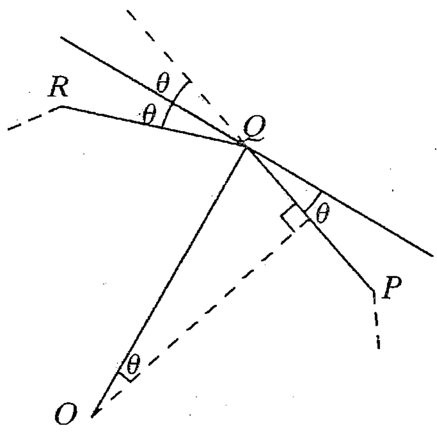
where M is the total mass of the gas.

This article is, however, concerned with the remarkable similarity between equation (1) and the circular motion relation

$$F = \frac{mv^2}{r}.$$

This provoked the following proof.

Consider a particle of mass m travelling around a regular n-sided polygon at a constant speed v. At each vertex a change in direction occurs, hence an impulse must act. In the diagram, the particle's motion is along PQR, Q is a vertex and $\theta = \pi/n$. The impulse acts towards O when the particle is at Q. The change in momentum is $2mv \sin\theta$ per collision, and so



$$2mnv \sin\theta \quad \text{per revolution.} \tag{2}$$

If the distance from all the vertices to O is r, then the time taken for one revolution around the polygon is given by

$$t = \frac{\text{perimeter}}{\text{speed}} = \frac{2nr \sin\theta}{v}. \tag{3}$$

By considering (2) and (3), we can see that the average rate of change of momentum is

$$\frac{2mnv \sin\theta}{(2nr \sin\theta)/v} = \frac{mv^2}{r}.$$

As $n \to \infty$ the motion of the particle approaches that of a circle with centre O and radius r. The particle's direction of motion is changing continuously, so the impulse acts continuously. Hence

$$F = \frac{\mathrm{d}}{\mathrm{d}t}(mv) = \frac{mv^2}{r}.$$

As all the impulses are directed towards O, this force is also acting towards O, as required. For a physical interpretation of this explanation, imagine a ball bouncing around a circular billiard table.

The connection with the gas-law relation is now easily explained. Consider the particle to be moving backwards and forwards along a diameter of a circle. Each collision requires a momentum transfer of $2mv$, and a collision occurs every $2r/v$ units of time. So the force (momentum per unit time) is mv^2/r.

An Integral of Ramanujan's

L. SHORT, *Napier University*

The author lectures at Napier University in Edinburgh and has fairly wide mathematical interests. These include the behaviour of simple iterative systems, the (sadly neglected) subject of continued fractions and the historical evolution of mathematical ideas.

Srinivasa Ramanujan (1887–1920) is justly famous for producing remarkable (and at times bewildering) formulae apparently from nowhere. Many of his results involve infinite series and require advanced analysis, but some can be discussed with elementary methods. Recently I came across the following integral (see the reference):

$$\int_0^\infty \frac{1}{(x^2+11^2)(x^2+21^2)(x^2+31^2)(x^2+41^2)(x^2+51^2)}\,\mathrm{d}x$$

$$= \frac{5\pi}{12\times13\times16\times17\times18\times22\times23\times24\times31\times32\times41}. \quad (1)$$

Attempting to verify this result leads to a variety of formulae along similar lines.

If we generalize the integral in (1) and define

$$I(a_1,a_2,\dots,a_n) = \int_0^\infty \frac{1}{(x^2+a_1^2)(x^2+a_2^2)\cdots(x^2+a_n^2)}\,\mathrm{d}x, \tag{2}$$

where $a_1,a_2,\dots,a_n > 0$, we can avoid cumbersome partial fraction expansions by noting that

$$\begin{aligned}
&I(a_1,\dots,a_n)-I(a_2,\dots,a_{n+1})\\
&\quad= \int_0^\infty \left(\frac{1}{(x^2+a_1^2)\cdots(x^2+a_n^2)} - \frac{1}{(x^2+a_2^2)\cdots(x^2+a_{n+1}^2)}\right)\mathrm{d}x\\
&\quad= \int_0^\infty \frac{(x^2+a_{n+1}^2)-(x^2+a_1^2)}{(x^2+a_1^2)\cdots(x^2+a_{n+1}^2)}\,\mathrm{d}x\\
&\quad= (a_{n+1}^2-a_1^2)\,I(a_1,\dots,a_{n+1}).
\end{aligned}$$

Hence we obtain the simple recurrence relation, for $a_1 \neq a_{n+1}$,

$$I(a_1,\dots,a_{n+1}) = \frac{1}{a_{n+1}^2-a_1^2}[I(a_1,\dots,a_n)-I(a_2,\dots,a_{n+1})], \tag{3}$$

together with the starting value

$$I(a_1) = \int_0^\infty \frac{1}{x^2+a_1^2}\,\mathrm{d}x = \frac{1}{a_1}\left[\tan^{-1}\frac{x}{a_1}\right]_0^\infty = \frac{\pi}{2a_1}. \tag{4}$$

From (3) and (4) we readily obtain the expressions

$$\begin{aligned}
I(a_1,a_2) &= \frac{\pi}{2a_1a_2(a_1+a_2)},\\
I(a_1,a_2,a_3) &= \frac{\pi(a_1+a_2+a_3)}{2a_1a_2a_3(a_1+a_2)(a_2+a_3)(a_1+a_3)},\\
I(a_1,\dots,a_4) &= \frac{\pi[(a_1+a_4)(a_1+a_2+a_3)(a_2+a_3+a_4)+a_2a_3(a_2+a_3)]}{2a_1a_2a_3a_4(a_1+a_2)(a_1+a_3)(a_1+a_4)(a_2+a_3)(a_2+a_4)(a_3+a_4)}.
\end{aligned} \tag{5}$$

The expression for $I(a_1,\dots,a_5)$ is somewhat complicated in its general form, but, in any particular case, is easily generated from the result for $I(a_1,\dots,a_4)$ via (3).

An interesting special case of (5) arises when the a_i's are in arithmetic progression, i.e.

$$a_i = a+(i-1)\,d. \tag{6}$$

This leads to the following expressions:

$$\begin{aligned}
I(a,a+d) &= \frac{\pi}{2a(a+d)(2a+d)}, \\
I(a,a+d,a+2d) &= \frac{3\pi}{2a(a+2d)(2a+d)(2a+2d)(2a+3d)}, \\
I(a,\ldots,a+3d) &= \frac{5\pi}{a(a+3d)(2a+d)(2a+2d)(2a+3d)(2a+4d)(2a+5d)}, \\
I(a,\ldots,a+4d) &= \\
&\frac{35\pi}{a(2a+d)(2a+2d)(2a+3d)(2a+4d)(2a+5d)(2a+6d)(2a+7d)(2a+8d)}.
\end{aligned} \tag{7}$$

Equation (1) follows directly from the final result in (7) with the choice $a = 11$ and $d = 10$. Many further results along these lines can be obtained from (5) and (7). For example,

$$\int_0^\infty \frac{1}{(x^2+3^2)(x^2+4^2)(x^2+5^2)}\,dx = \frac{\pi}{7\times8\times9\times10},$$

$$\int_0^\infty \frac{1}{(x^2+27^2)(x^2+37^2)(x^2+47^2)(x^2+57^2)}\,dx =$$

$$\frac{5\pi}{2^5\times27\times32\times37\times42\times47\times52\times57}.$$

Another example along the lines of (1) is the following amazing result (see the reference):

$$\int_0^\infty \frac{1}{(1+x^2)(1+0.001x^2)(1+0.00001x^2)\cdots}\,dx = \frac{\pi}{2.202002000200002\ldots}.$$

But this is rather difficult to prove.

Reference

D. Castellanos, 'The ubiquitous π', *Math. Mag.* **61** (1988), 67–98.

1992

Eleven distinct numbers are chosen in order from the numbers 1, 2, 3, ..., 22 reduced modulo 2 (i.e. written as 0 if even and 1 if odd) and written down in a list from left to right. What is the probability that the number obtained is the year 1992 written in base 2?

FARSHID ARJMANDY
(A student of computer engineering at Shareef University, Tehran)

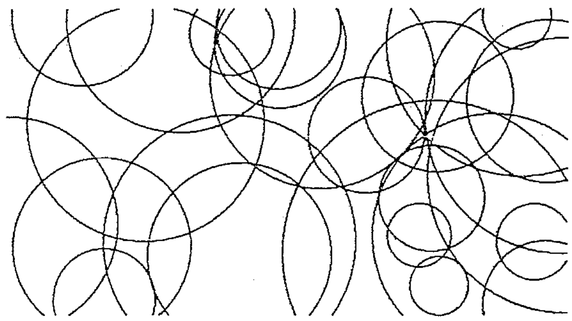
Computer Column

MIKE PIFF

Bresenham's circle drawing algorithm

In the last column we addressed the problem of drawing a straight line between two points. We shall now see how to draw a circle given its centre and radius.

Bresenham devised the following algorithm to draw a circle. It can be included in the module `graphics` for use in any of your modules. However, it is safer to include the following slight modification of *PutPixel*, which checks to see that the point is within the screen boundaries. The values of *ScreenRows* and *ScreenCols* must be adjusted to the resolution you are using.



```
CONST
  ScreenRows=349;  ScreenCols=639;
PROCEDURE PutPixel(column, row,
  colour:INTEGER);
BEGIN
 IF (column≥0)AND
   (column≤ScreenCols)AND
    (row≥0)AND
     (row≤ScreenRows) THEN
   CX:=column; DX:=row;
   AX:=plotfn×high+colour;
   BX:=high×Page; Trap(GraphInt);
 END;
END PutPixel;
PROCEDURE Circle(cx, cy, R,
colour:INTEGER);
VAR
 dist, temp, x, y:INTEGER;
 PROCEDURE MoveE;
 BEGIN
  x:=x+1;
  dist:=dist+2×x+1;
 END MoveE;
 PROCEDURE MoveSE;
 BEGIN
  x:=x+1; y:=y-1;
  dist:=dist+2×x-2×y+2;
 END MoveSE;
 PROCEDURE MoveS;
 BEGIN
  y:=y-1;
  dist:=dist-2×y+1;
 END MoveS;
BEGIN
 x:=0;
 y:=R;
 dist:=2×(1-R);
 LOOP
  PutPixel(cx+x,cy+y,colour);
  PutPixel(cx+x,cy-y,colour);
  PutPixel(cx-x,cy+y,colour);
  PutPixel(cx-x,cy-y,colour);
  IF y=0 THEN EXIT; END;
  IF dist>0 THEN
   temp:=2×dist-2×x-1;
   IF temp>0 THEN
    MoveS;
   ELSE
    MoveSE;
   END;
  ELSIF dist<0 THEN
   temp:=2×dist+2×y-1;
   IF temp>0 THEN
    MoveSE;
   ELSE
    MoveE;
   END;
  ELSE
   MoveSE;
  END;
 END;
END Circle;
```

Letter to the Editor

Dear Editor,

$$x^3+y^3 = z^2$$

Mordell (page 235) lists the families of integer solutions to this equation for which $(x,y) = 1$ and y is odd. Clearly, if x and y have a common factor d then d also divides z but, since the equation is inhomogeneous, we may not be able to cancel it from x and y.

Following my earlier letter in *Mathematical Spectrum* (Volume 24, Number 3, page 88), I have observed that there is a family of rational solutions given by

$$\left(\frac{u+v}{2u(u^2+3v^2)}\right)^3+\left(\frac{u-v}{2u(u^2+3v^2)}\right)^3 = \left(\frac{1}{2u(u^2+3v^2)}\right)^2,$$

where u and v are integers. (If u, v are rational we can multiply up by their common denominator.)

For example, $u = 3$, $v = 1$ leads to $4^3+2^3 = 72$ or

$$2^3+1^3 = 3^2$$

and $u = 3$, $v = 2$ leads to

$$5^3+1^3 = 2\times3\times21 = 2\times3^2\times7$$

so that

$$(2\times5\times7)^3+(1\times2\times7)^3 = 2^4\times3^2\times7^4 = (2^2\times3\times7^2)^2,$$

i.e.

$$70^3+14^3 = 588^2.$$

In general the identity becomes

$$(u+v)^3+(u-v)^3 = 2u(u^2+3v^2).$$

For each prime p that divides $2u(u^2+3v^2)$ to an odd exponent we multiply both sides of the equation by p^3 to end up with a solution to $x^3+y^3 = z^2$.

Note that, with $x = 70$, $y = 14$, $x+y$ is neither a square nor three times a square as suggested by K. R. S. Sastry's results in Volume 21, Number 3, pages 98–99.

Reference

L. J. Mordell, *Diophantine Equations* (Academic Press, New York, 1969).

Yours sincerely,
P. Young
(79 Gladstone Street,
Beeston,
Nottingham NG9 1FP)

Problems and Solutions

Sixth formers and 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 may qualify 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

25.4 (Submitted by Peter Mason, a student at the University of Warwick)
Evaluate

$$\int_0^1 \ln(1+x)\ln(1-x)\ dx.$$

$$\left[\text{Hint:}\quad \sum_{n=1}^{\infty}\frac{1}{n^2} = \tfrac{1}{6}\pi^2.\right]$$

25.5 (Submitted by A. Y. Özban, Karadeniz Technical University, Turkey)
For a natural number n, denote by $T(n)$ the sum of its digits when written in decimal form, and define

$$S(n) = \begin{cases} T(n) & (\text{if } T(n) \leqslant 9), \\ S(T(n)) & (\text{if } T(n) > 9). \end{cases}$$

Determine (i) $S(2^p)$ when p is prime and $p > 3$ and (ii) $\displaystyle\sum_{k=1}^{\infty}\frac{S(2^{k-1})}{2^k}$.

25.6 (Submitted by Dermot Roaf, Exeter College, Oxford—see his article in this issue)
Find the angles subtended at the centre by non-adjacent vertices in a dodecahedron and in an icosahedron.

Solutions to Problems in Volume 24 Number 4

24.10 Obtain a formula for the sum of the cubes of n integers in arithmetic progression.

Solution by Sumita Kumar (National University of Lesotho)
Write $u_r = a+(r-1)d$. Then

$$\begin{aligned}\sum_{r=1}^{n} u_r^3 &= a^3\sum_{r=1}^{n} 1 + 3a^2d\sum_{r=1}^{n}(r-1) + 3ad^2\sum_{r=1}^{n}(r-1)^2 + d^3\sum_{r=1}^{n}(r-1)^3 \\ &= na^3 + 3a^2d\tfrac{1}{2}n(n-1) + 3ad^2\tfrac{1}{6}n(n-1)(2n-1) + d^3[\tfrac{1}{2}n(n-1)]^2.\end{aligned}$$

Also solved by Mark Blyth (Gresham's School, Holt) and Amites Sarkar (Trinity College, Cambridge).

24.11 Evaluate

$$\int_0^{\frac{1}{2}\pi} \frac{\cos^4 x}{\sqrt{2}-\sin 2x}\,dx.$$

Solution by Peter Mason
Denote the integral by I. We substitute $x = \frac{1}{2}\pi - y$ to give

$$I = \int_{\frac{1}{2}\pi}^{0} \frac{\sin^4 y}{\sqrt{2}-\sin(\pi-2y)}(-dy) = \int_0^{\frac{1}{2}\pi} \frac{\sin^4 y}{\sqrt{2}-\sin 2y}\,dy,$$

so that

$$I = \tfrac{1}{2}\int_0^{\frac{1}{2}\pi} \frac{\cos^4 x+\sin^4 x}{\sqrt{2}-\sin 2x}\,dx.$$

Now

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

so that

$$\begin{aligned}I &= \tfrac{1}{4}\int_0^{\frac{1}{2}\pi}(\sqrt{2}+\sin 2x)\,dx\\ &= \tfrac{1}{4}\Big[x\sqrt{2}-\tfrac{1}{2}\cos 2x\Big]_0^{\frac{1}{2}\pi}\\ &= \tfrac{1}{8}(\pi\sqrt{2}+2).\end{aligned}$$

Also solved by Mark Blyth and Amites Sarkar.

24.12 (The problem referred to cyclotomic polynomials described in Volume 24 Number 4, pages 105–107.) Show that

(i) $\phi_{2p}(x) = \phi_p(-x)$, where p is an odd prime;

(ii) $\phi_{2pq}(x) = \phi_{pq}(-x)$, where p and q are distinct odd primes;

(iii) if $r = p^n$, where p is prime and n is a positive integer, then $\phi_r(1) = p$, but that, for all other values of r greater than 1, $\phi_r(1) = 1$.

Solution by Amites Sarkar

(i)
$$\begin{aligned}\phi_{2p}(x)\phi_p(x)\phi_2(x)\phi_1(x) &= x^{2p}-1\\ &= (x^p+1)(x^p-1)\\ &= -[(-x)^p-1](x^p-1)\\ &= -\phi_p(-x)\phi_1(-x)\phi_p(x)\phi_1(x)\\ &= \phi_p(-x)\phi_p(x)\phi_2(x)\phi_1(x),\end{aligned}$$

so that $\phi_{2p}(x) = \phi_p(-x)$.

(ii) $\phi_{2pq}(x)\phi_{2p}(x)\phi_{2q}(x)\phi_2(x)\phi_{pq}(x)\phi_p(x)\phi_q(x)\phi_1(x)$

$$\begin{aligned}
&= x^{2pq}-1\\
&= (x^{pq}+1)(x^{pq}-1)\\
&= -[(-x)^{pq}-1](x^{pq}-1)\\
&= -\phi_{pq}(-x)\phi_p(-x)\phi_q(-x)\phi_1(-x)\phi_{pq}(x)\phi_p(x)\phi_q(x)\phi_1(x)\\
&= \phi_{pq}(-x)\phi_{2p}(x)\phi_{2q}(x)\phi_2(x)\phi_{pq}(x)\phi_p(x)\phi_q(x)\phi_1(x),
\end{aligned}$$

so that $\phi_{2pq}(x) = \phi_{pq}(-x)$.

(iii) For $r = p^n$, p prime and n a positive integer,

$$\begin{aligned}
&\phi_r(x)\phi_{p^{n-1}}(x)\phi_{p^{n-2}}(x)\cdots\phi_p(x)\phi_1(x)\\
&= x^r-1\\
&= (x^{p^{n-1}}-1)(x^{(p-1)p^{n-1}}+x^{(p-2)p^{n-1}}+\cdots+1)\\
&= (x^{(p-1)p^{n-1}}+x^{(p-2)p^{n-1}}+\cdots+1)\phi_{p^{n-1}}(x)\phi_{p^{n-2}}(x)\cdots\phi_p(x)\phi_1(x),
\end{aligned}$$

so that

$$\phi_r(x) = x^{(p-1)p^{n-1}}+x^{(p-2)p^{n-1}}+\cdots+1$$

and $\phi_r(1) = p$.

If $r > 1$ and r is not a prime power, then we can write $r = ab$ with $a > 1$, $b > 1$ and a and b coprime. Now we have

$$\begin{aligned}
\prod_{d|r}\phi_d(x) &= x^{ab}-1\\
&= (x^a-1)(x^{(b-1)a}+x^{(b-2)a}+\cdots+1)\\
&= (x^{(b-1)a}+x^{(b-2)a}+\cdots+1)\prod_{d|a}\phi_d(x),
\end{aligned}$$

which gives

$$\prod_{d|r,\, d\nmid a}\phi_d(x) = x^{(b-1)a}+x^{(b-2)a}+\cdots+1.$$

Similarly,

$$\prod_{d|r,\, d\nmid b}\phi_d(x) = x^{(a-1)b}+x^{(a-2)b}+\cdots+1.$$

From these we have

$$\prod_{d|r,\, d\nmid a}\phi_d(1) = b, \qquad \prod_{d|r,\, d\nmid b}\phi_d(1) = a.$$

Each of these products is a product of integers, as all coefficients of cyclotomic polynomials are integers. Since r certainly divides r, but r divides neither a nor b, we see that $\phi_r(1)$ divides both a and b. But a and b are coprime. Hence $\phi_r(1) = 1$.

Peter Mason also solved (i), (ii) and the first part of (iii).

Amites Sarkar points out that (i) and (ii) can be generalised to $\phi_{2n}(x) = \phi_n(-x)$ for n odd and $n > 1$—see Garling's *Galois Theory* (Cambridge University Press, 1986), page 120, where this is posed as an exercise. Amites Sarkar's proof of this is by complete induction on n. Consider a particular $n > 1$. Then

$$\prod_{d|n} \phi_{2d}(x)\phi_d(x) = x^{2n}-1 = -\{(-x)^n-1\}\{x^n-1\}$$

so that

$$\prod_{d|n} \phi_{2d}(x) = -\{(-x)^n-1\} = -\prod_{d|n} \phi_d(-x).$$

By the inductive assumption, $\phi_{2d}(x) = \phi_d(-x)$ for $d|n$, $d > 1$ and $d \neq n$. Also $\phi_2(x) = x+1 = -\phi_1(-x)$. Hence $\phi_{2n}(x) = \phi_n(-x)$. This completes the induction. (Note that this argument shows that $\phi_6(x) = \phi_3(-x)$, which is the case $n = 3$.)

Reviews

The Unexpected Hanging and Other Mathematical Diversions. By MARTIN GARDNER. The University of Chicago Press, 1991. Pp. 263. Paperback £8.75 (ISBN 0-226-28256-2).

This is a collection of puzzles, problems and paradoxes expanded and updated from Gardner's *Scientific American* column. The book takes you on a journey through all manner of fields from 'Knots and Borromean Rings' to 'Peg Solitaire'. Those familiar with Martin Gardner's writings will no doubt be aware of the diversity and richness of his works, and this book certainly continues in that vein.

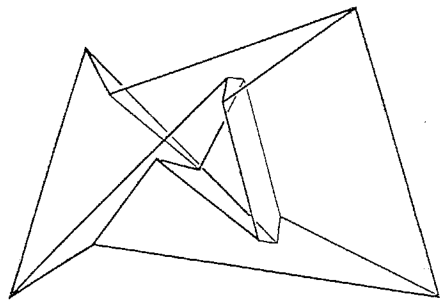
Chapters I found to be particularly interesting were 'The paradox of the unexpected hanging' and 'The transcendental number e'. The former is a wonderful mind-twister which has challanged both the philosopher and the mathematician and leaves you feeling mentally exhausted if you think too hard about it. The latter is a short chapter full of curiosities concerning the 'magical' number e. Other chapters will no doubt be preferred by other readers, but there is something here for everyone.

The book finishes with a chapter of 37 catch questions to keep you on your toes, and these are a great deal of fun to answer. There is an afterword by Gardner which attempts to tie up a few loose ends, and a bibliography crammed with relevant references.

Gardner fans will not be disappointed by this book, and I would recommend it to anyone looking for an entertaining and thought-provoking book to read in their spare time.

Sixth form, Richard Hale School, Hertford MATTHEW PHILLIPS

Fractal Music, Hypercards and More. By MARTIN GARDNER. W. H. Freeman, Oxford, 1991. Pp. 327. Paperback £10.95 (ISBN 0-7167-2189-9).



The Szilassi toroidal polyhedron has the property that any two faces share a common edge (from page 119).

Those familiar with Martin Gardner's writing will require no introduction to this book. It is the fourteenth collection from the Mathematical Games column of *Scientific American*, covering the years 1978 and 1979. The columns cross a broader range than their title would suggest. As well as discussion about a host of novel games, there are chapters on geometric problems, number theory, essays on philosophy, music, sculpture, and a review of *Gödel, Escher, Bach*. The style is clear and simple throughout—no technical mathematics is used (every use of factorial '!' is explained!). And yet the book does not lack substance. From the basics Gardner goes on to describe the results of eminent mathematicians. Most chapters contain one or two 'set' problems whose answers are given at the end.

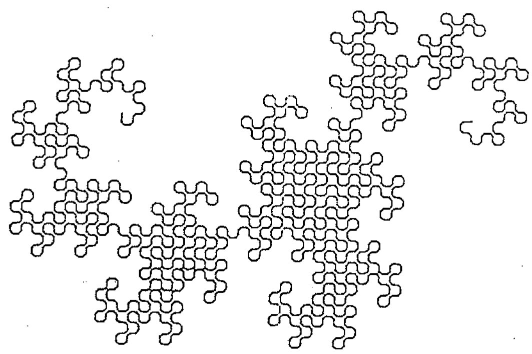
The last chapter is my favourite: an essay on Chaitin's Omega. This constant is the probability that a Turing machine stops when given random data. It turns out that the answers to most interesting problems in mathematics lie in the first 5000 binary digits of Omega! To conclude, I would recommend this book strongly to anyone whose interest in mathematics goes beyond the blackboard, which is most people reading this magazine.

Trinity College, Cambridge — DYLAN GOW

Fractals: Endlessly Repeated Geometrical Figures. By HANS LAUWERIER. Penguin, London, 1991. Pp. xiv+209. Paperback £9.99 (ISBN 0-14-014411-0).

This book has a very practical flavour. Nearly all the fractals discussed have a BASIC generating program listed in the back. Many of these use efficient low-memory techniques, and none requires a recursive procedure facility. In addition there are a few fractal-designing programs. Programming methods are well explained in the main text.

The book kicks off its description of fractals with an explanation of 'fractal dimension', using the amazing example of the west coast of Britain. A variety of geometric fractals is then introduced: dust clouds, meanders, trees, dendrites. More 'natural'-looking fractals are produced using random factors. Interest next shifts to the study of iterative formulae, which can be used to model a wide range of natural phenomena: population growth, celestial mechanics, even particles in particle accelerators. Fractals rear their heads in the structure of the orbits of such iterations. Stability, strange attractors and Feigenbaum's number are other terms explained. Finally, we are led to the more abstract side of iterative forms: Julia sets and, lastly, the ubiquitous Mandelbrot set.



This is an excellent introduction, suitable for A-level students in mathematics, art or computer science. Little mathematical knowledge is assumed: there are chapters on number systems and complex numbers. There are plenty of diagrams and colour plates. My favourite is the dragon curve on page 52. This can be made by folding a long strip of paper repeatedly, then unfolding. Notice how the curve never crosses itself.

Trinity College, Cambridge DYLAN GOW

A Mathematician's Apology. By G. H. HARDY. Cambridge University Press, 1992. Pp. 153. Paperback £4.95 (ISBN 0-521-42706-1).

This is a reprint of a classic of mathematical literature. G. H. Hardy was one of the great mathematicians of his day and, fortunately for later generations, he set out in his *Apology* his attitude to mathematics and what motivated him to do it. This is prefaced in the present volume by a fascinating glimpse into the man himself by his contemporary, the novelist C. P. Snow. Although some of Hardy's comments, in particular those on the usefulness or otherwise of mathematics, may now seem dated, they do not detract from the enduring fascination of this volume, which is a must for all aspiring mathematicians.

University of Sheffield D. W. SHARPE

Other books received

Index to Mathematical Problems 1980–1984. Edited by STANLEY RABINOWITZ. MathPro Press, Westford, MA, 1992. Pp. xii+532. Hardback $49.95 (ISBN 0-9626401-1-5).

This large volume is a compilation of problems (minus solutions) which appeared from 1980 to 1984 in magazines and journals like *Mathematical Spectrum* which have problem sections. They are catalogued according to the subject matter. A useful reference work for anyone looking for more challenging and out-of-the-ordinary problems.

Mathematical Byways. By HUGH APSIMON. Oxford University Press, 1991. Pp. vi+97. Paperback £6.99 (ISBN 0-19-286137-9).

This is the paperback edition of a book first published in hardback in 1984.

Functional Analysis: A Primer. By LAWRENCE W. BAGGETT. Marcel Dekker, New York, 1992. Pp. xi+267. Hardback $49.75. (ISBN 0-8247-8598-3).

The Puzzling World of Polyhedral Dissections. By STEWART T. COFFIN. Oxford University Press, 1991. Pp. 196. Paperback £8.99 (ISBN 0-19-286133-6).

The hardback version of this book was reviewed in Volume 24, Number 1, page 30.

Probability: The Mathematics of Uncertainty. By DORIAN FELDMAN AND MARTIN FOX. Marcel Dekker, New York, 1992. Pp. xv+404. Hardback $155.25. (ISBN 0-8247-8452-9).

A Basic Course in Statistics. By G. M. CLARKE AND D. COOKE. Edward Arnold, London, 1992, third edition. Pp. xx+451. Paperback £13.99 (ISBN 0-340-56772-4).

Lectures on Partial Differential Equations. By I. G. PETROVSKY. Dover, New York, 1992. Pp. x+245. Paperback £7.95 (ISBN 0-486-66902-5).

This Dover edition, first published in 1991, is a republication of the work first published by Interscience Publishers, New York, in 1954.

The Penguin Dictionary of Information Technology and Computer Science. By TONY GUNTON. Penguin Books, London, 1992. Pp. 205. Paperback £5.99. (ISBN 0-14-051240-3).

First Published by NCC Blackwell, 1990.

Work Out Statistics A-level. By A. D. BALL AND G. D. BUCKWELL. Macmillan Education, Basingstoke, 1992, third edition. Pp. xii+265. Paperback £7.50 (ISBN 0-333-56333-6).

Matrix Algebra. By DAVID J. WINTER. Macmillan, New York, 1992. Pp. xvi+540. (ISBN 0-02-428831-4).

Discrete Mathematics for Computing. By JOHN E. MUNRO. Chapman and Hall, London, 1992. Pp. x+306. £16.95 (ISBN 0-412-45650-8).

Dynamical Systems: Differential Equations, Maps and Chaotic Behaviour. By D. K. ARROWSMITH AND C. M. PLACE. Chapman and Hall, London, 1992. Pp. x+330. Paperback £17.95 (ISBN 0-412-39080-9).

This book is for second- and third-year undergraduates and for graduate students, and covers the developing area of chaos and fractals within the context of teaching differential equations.

A Survey of Matrix Theory and Matrix Inequalities. By MARVIN MARCUS AND HENRY MINC. Dover, New York, 1992. Pp. xii+180. Paperback £5.95 (ISBN 0-486-67102-X).

This Dover edition is a republication of the corrected (1969) printing of the work first published by Prindle, Weber and Schmidt, Boston, 1964, as Volume 14 of 'The Prindle, Weber and Schmidt Complementary Series in Mathematics'.

Mary Rose

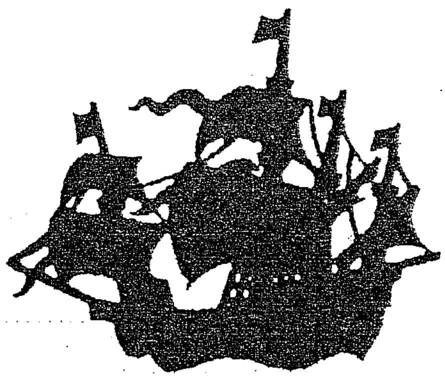
PORTSMOUTH

6000 children have now visited the new Maths + Science = Mary Rose display at the Mary Rose, in Portsmouth's historic dockyard. Since it opened in October 1991 it has proved so popular that it is to be extended to spring term 1993.

Free to pre-booked school parties the display explores some of the problems associated with underwater excavation, salvage and presentation of the Tudor warship and her contents. Pupils can test their dexterity in raising and lowering a yard-arm on a nine-foot-high model of the main mast. They can use computer software to search, excavate and recover artefacts hidden in the ship. Other parts of the display include a ship-loading puzzle, a Tudor sailing game and an examination of the dangers of exposing some materials to sunlight.

An accompanying educational pack (price £2.50 + 75p postage and packing) combines museum-based activities with a range of exercises and experiments that can be carried out in the classroom.

For more information concerning visits contact Barbara Barnes on 0705 812931. For information on educational content contact the Trust's Research and Interpretation Department on 0705 750521.



CONTENTS

ISSN 0025-5653

PRICES (*postage included*)
Prices for Volume 25 (Issues Nos. 1, 2, 3 and 4)

£7.00 or US$12.30 or $A16.20

These prices apply to subscribers in all parts of the world. There is now only one set of sterling rates applicable to all countries.

A discount of 10% will be allowed on all orders of five or more copies of Volume 25 sent to the same address.

Details of reduced prices for two- and three-year subscriptions available on request.

Back issues

All back issues except Volume 1 are available; information concerning prices and a list of the articles published may be obtained from the Editor.

Enquiries about rates, subscriptions and advertisements should be directed to:

Editor—Mathematical Spectrum,
Hicks Building,
The University,
Sheffield S3 7RH, UK.

Published by the Applied Probability Trust
Typeset by The Pi-squared Press, Nottingham, UK
Printed by Galliard (Printers) Ltd, Great Yarmouth, UK