MATHEMATICAL SPECTRUM

A MAGAZINE FOR STUDENTS AND TEACHERS OF MATHEMATICS AT SCHOOLS, COLLEGES AND UNIVERSITIES

Volume 21 1988/89 Number 1

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 21 of *Mathematical Spectrum* will consist of three issues, of which this is the first. The second will be published in January 1989 and the third in May 1989.

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 copyright of all published material is vested in the Applied Probability Trust.

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

Cryptographic Uses of Large Numbers

FRED PIPER, *Royal Holloway and Bedford New College*

Fred Piper is Professor of Mathematics at Royal Holloway and Bedford New College, a part of the University of London. He enjoys lecturing and writing articles on cryptography at levels ranging from 12-year-old schoolchildren to international conferences for professionals.

1. Introduction

In a recent article in *Mathematical Spectrum* (reference 7) Ian Stewart discussed the difficulties of factorizing large numbers. In this article we show how these difficulties are being exploited in modern cryptography. We also show how cryptographers are exploiting the difficulty of another problem associated with large numbers, namely that of finding discrete logarithms with a large modulus (these terms are defined in section 2).

Figure 1 shows a typical convention (or symmetric) cipher system. The assumption is that A wishes to send a message to B but A disguises it so that it is unintelligible to anyone who intercepts it. In order to achieve this objective A and B have to agree (prior to sending the message) on the algorithm which is going to be used to disguise the message. Since the interceptor is likely to know the algorithm being used, A and B must also agree on a key, which they must keep secret. It is lack of knowledge of this key which prevents the interceptor from obtaining m from c. Mathematically A has a family of functions from which he selects one which depends on the agreed key k. If we denote this function by f_k then $c = f_k(m)$. Since B knows k, B knows that f_k is being used and then uses f_k^{-1} to obtain m from c.

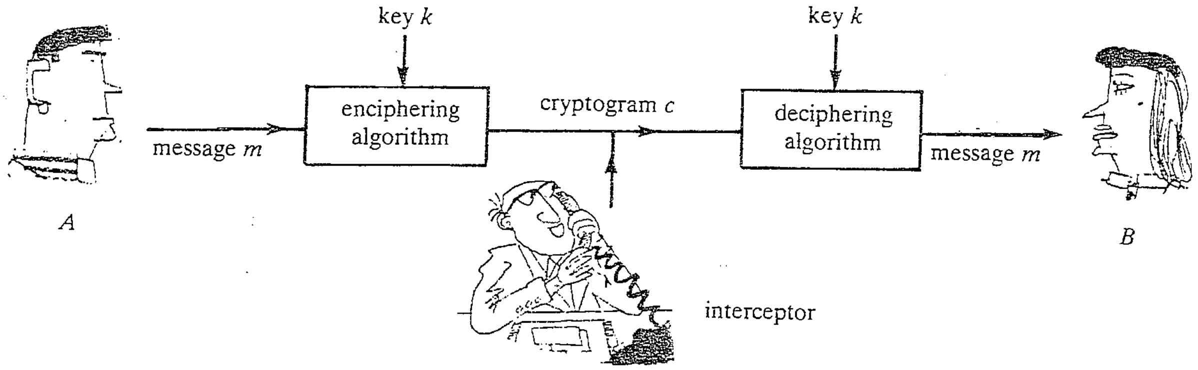


Figure 1

We illustrate with a very simple (and insecure!) example. The letters A to Z are assigned the numbers 0 to 25 respectively and the algorithm is addition mod 26. The key k might be an integer which is to be added and thus k can be any integer from 1 to 25. (Note that nothing is achieved by adding 0.) Thus, for example, if the key is $k = 5$ and the message is CAT, then the cryptogram is HFY.

Anyone interested in understanding the general principles of conventional cryptography should consult either reference 1 or reference 2. For this article the only important fact is that the communicators need to have agreed on an algorithm and a key before they can exchange secret messages. Since the secrecy of the message depends upon the secrecy of the keys, these initial keys must be distributed secretly. But how? This is clearly a potentially difficult problem and is one of the major 'headaches' of conventional cryptography.

In 1976 Diffie and Hellman published an innovative paper, aptly named 'New directions in cryptography' (reference 3), which has had a fundamental influence on modern cryptography. In it they suggested a method for overcoming the initial key distribution problem. Their scheme is discussed in section 2. In the same paper they also proposed the use of asymmetric or public key systems. In these systems the keys used by the encipherer and decipherer are different and, furthermore, it is extremely difficult to deduce the deciphering key from the enciphering key. One example of this type of system is the RSA public key system, which exploits the difficulty of factorizing large numbers. We discuss this in section 3.

2. The Diffie–Hellman key exchange scheme

We begin our discussion of this scheme by illustrating it with a small example. We assume that two people, A and B say, wish to be in the position where they have some common secret knowledge (in the form of a number). Furthermore we assume that, in order to achieve this, they have to communicate in public, i.e. that everybody knows exactly what they are doing. We stress that A and B are not enciphering messages, they are merely agreeing on a secret number which they can then use as the key to encipher and/or decipher a message.

Before working through the example we must point out that, prior to the Diffie–Hellman paper (1976), it had been commonly assumed that it was impossible to agree secret information in public, unless the 'machinery' had been agreed beforehand. Thus the simplicity of the Diffie–Hellman scheme is remarkable.

We divide our example into a number of steps.

Step 1 A chooses a large prime p and an integer n which is less than p. (There are, as we shall see later, some optimal choices for n once p is chosen.) For our example we assume that A chooses $p = 101$ and $n = 12$. These numbers are too small to offer any secrecy but are chosen merely to indicate the procedure.

Step 2 A publicly tells B the values of p and n. Thus everyone knows that $p = 101$ and $n = 12$.

Step 3 A thinks of a number a (which he keeps secret) and tells B to think of a number b and keep it secret. For our example we assume A chooses $a = 8$ and that B chooses $b = 19$. It is important to note that A does not know that value of b and B does not know a. Thus A and B do not need to trust each other.

Step 4 A computes $n^a \pmod{p}$ and tells B to compute $n^b \pmod{p}$. For our example:

$$12^8 \equiv 52 \pmod{101}, \qquad 12^{19} \equiv 50 \pmod{101}.$$

Here we remind the reader that $n^a \pmod{p}$ is the remainder when n^a is divided by p. For this small example computing $n^a \pmod{p}$ is easy, but for larger numbers it is not quite so straightforward (see the discussion in section 3).

Step 5 A publicly tells B the value of $n^a \pmod{p}$ and B publicly tells A the value of $n^b \pmod{p}$. Thus everybody knows the values of $n^a \pmod{p}$ and $n^b \pmod{p}$ which, for our example, are 52 and 50, respectively.

Step 6 A raises B's number to the power a and reduces modulo p, i.e., A computes $(n^b)^a \pmod{p}$ which, for our example is $50^8 \pmod{101}$. He then tells B to raise A's number to the power b and reduce modulo p, i.e., B computes $(n^a)^b \pmod{p}$ which, for our example, is $52^{19} \pmod{101}$.

At the end of these 6 steps, A has $(n^b)^a \pmod{p}$ and B has $(n^a)^b \pmod{p}$. Since both of these numbers are $n^{ab} \pmod{p}$, A and B now have the same value. In our example this number is $50^8 \pmod{101}$ or $52^{19} \pmod{101}$ which is 58. Note, by the way, that since A does not know the number used by B, and vice versa, neither A nor B could have predicted in advance what the answer would be. Hence our earlier assertion that this technique cannot be used for sending secret messages.

It should be clear that, whatever values are chosen for a and b, A and B will always end up with the same number. However, it may not be quite so obvious that the number cannot be deduced by anyone listening to their conversations. If we consider our example, then any eavesdropper will know that $p = 101$, $n = 12$, $12^a \equiv 52 \pmod{101}$ and $12^b \equiv 50 \pmod{101}$. Thus if the eavesdropper can solve one of the equations $12^a \equiv 52 \pmod{101}$ or $12^b \equiv 50 \pmod{101}$ for a or b, he will then be able to compute either $52^b \pmod{101}$ or $50^a \pmod{101}$ to obtain the (supposedly secret) final value of 58.

But how do you solve an equation of the form $12^b \equiv 50 \pmod{101}$? Try it. You will almost certainly end up systematically trying values for b until you find the one which works. This is feasible for the size of number which we have used in our example. However, as the values of b and the modulus get larger, you will find that the time taken increases rapidly. [Try solving $13^x \equiv 133 \pmod{523}$ if you need convincing!]

When we described Step 1 we said that there were optimal choices for n once p is chosen. To see why, we shall, once again, look at a small example. If we put $p = 13$, then table 1 shows all possible values for $n^x \pmod{p}$ for each possible choice of n.

Table 1

Value of n	Powers of n modulo 13
1	1
2	2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1
3	3, 9, 1
4	4, 3, 12, 9, 10, 1
5	5, 12, 8, 1
6	6, 10, 8, 9, 2, 12, 7, 3, 5, 4, 11, 1
7	7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2, 1
8	8, 12, 5, 1
9	9, 3, 1
10	10, 9, 12, 3, 4, 1
11	11, 4, 5, 3, 7, 12, 2, 9, 8, 10, 6, 1
12	12, 1

From this table we see, for instance, that $5^4 \equiv 1 \pmod{13}$ and thus if they had chosen $p = 13$ and $n = 5$ then there would be no point in either A choosing $a \geqslant 4$ or B choosing $b \geqslant 4$. (If for instance A chose $a = 14$ then, since $14 = 3 \times 4 + 2$, this would be the same as choosing $a = 2$.) The best values for n when $p = 13$ are, clearly, 2, 6, 7 or 11, since, for any one of these values, every non-zero integer modulo 13 is a power of n.

For a given prime p, any value n such that the integers 1 to $p-1$ are all powers of $n \pmod{p}$ is called a *primitive root* modulo p. Primitive roots exist for all primes, although there is no known efficient algorithm for finding them. In the Diffie–Hellman scheme n should be a primitive root modulo the prime p. If n is a primitive root modulo the prime p and if $y = n^x \pmod{p}$ then, for obvious reasons, x is called the *discrete logarithm* of y with respect to n.

3. The RSA public key cryptosystem

We now assume that we wish to set up a system so that anyone can send me a secret message. We shall do it in such a way that any two people who wish to send secret messages will perform exactly the same mathematical function but the function will be chosen in such a way that neither will be able to read the other's messages. Once again this was not conceived as possible until the celebrated Diffie–Hellman paper. The scheme here is the RSA scheme invented by Rivest, Shamir and Adleman (see reference 6).

We shall describe the procedure in a number of steps.

Step 1 We generate two large primes p and q which we keep secret.

Step 2 We compute $n = pq$.

Step 3 We choose h so that h and $(p-1)(q-1)$ have greatest common divisor 1.

Step 4 We compute d so that $dh \equiv 1 \pmod{(p-1)(q-1)}$. (This can be done because h and $(p-1)(q-1)$ have greatest common divisor 1.)

From Stewart's article we know that primality testing is straightforward and that there is a simple algorithm (Euclid's) for computing greatest common divisors. This same algorithm can be modified to compute d in Step 4.

Step 5 We publish n and h (but keep d secret).

Note that the published information is not sufficient to deduce d. It is certainly true that the algorithm for computing d is easy. However, as was stressed in Stewart's article, factoring large numbers is extremely hard and thus, provided n is large enough, we shall be the only people who know p and q. Without this knowledge it is impossible to determine the modulus for computing d.

Anyone wishing to send us a message could first use a standard code for converting it to binary and then change this to a string of integers which are all less than n. To send the integer m in 'secret' form they then compute $c \equiv m^h \pmod{n}$ and transmit c. Is this secure? Any interceptor will already know h and n (because they are public). Thus they will know h, n and $m^h \pmod{n}$ and will want to deduce m. However this is a difficult problem (not totally dissimilar to that discussed in the previous section!). In general unless the factors of n are known there is no feasible way of tackling it. (Again, if you need convincing try solving $m^{49} \equiv 3 \pmod{401}$.)

However we can utilize our knowledge of p and q to find m. (In fact this was why we computed d.) There is a well-known theorem (the Euler–Fermat theorem) which tells us that, if $n = pq$ and $k \equiv 0 \pmod{(p-1)(q-1)}$ then $x^k \equiv 1 \pmod{n}$ for all x with x and n coprime. This implies that $x^{k+1} \equiv x \pmod{n}$ for all x and so, in particular, $x^{hd} \equiv x \pmod{n}$ for all x. Thus, since $c \equiv m^h \pmod{n}$, $c^d \equiv m^{dh} \equiv m \pmod{n}$.

Clearly anyone who factors n can compute d and can therefore read our messages. However, Stewart's article showed that, provided n is large enough and p and q are chosen to resist certain specific factorization techniques (like, for instance, the Pollard technique quoted in Stewart's article), it is extremely unlikely that anyone will deduce p and q. Thus our messages should be secure.

We illustrate the RSA system with a small (again necessarily insecure!) example.

Step 1 Choose $p = 7$ and $q = 13$.

Step 2 $n = 91$.

Step 3 Choose $h = 7$. (Note: $(p-1)(q-1) = 72$ and 7 and 72 are coprime.)

Step 4 We must solve $7d \equiv 1 \pmod{72}$. The solution is $d = 31$. (This is easy to check!)

Step 5 We publish 91 and 7.

Anyone wishing to send a message could first convert it to binary, possibly using a standard code like ASCII, and then divide this binary sequence into blocks of 6 bits. Each block can now be written as a number from 0 to 63. (For obvious reasons precautions should be taken to ensure that 0 and 1 do not appear!) The message is now a sequence of integers all less than 91.

Suppose now that someone wishes to send the message $m = 54$. They then compute $c \equiv 54^7 \pmod{91}$. This gives $c = 89$. Thus they send the integer 89.

To decipher we compute $89^d \pmod{91} \equiv 89^{31} \pmod{91}$. The theory guarantees that this will equal 54; however, it might be interesting to check this and, at the same time show how to compute modular exponentiations easily.

If we were using a genuine RSA system, than all integers could be any size up to about 10^{160}. How, then, should we compute $m^h \pmod{n}$ or $c^d \pmod{n}$? We most certainly do not multiply m by itself h times and then reduce modulo n. (The size of m^h would be truly astronomic!) The first thing we note is that it is best to reduce all intermediate values modulo n. However, although this avoids our handling astronomical numbers, it does not help us reduce the number of multiplications. We shall compute $89^{31} \pmod{91}$ and leave the reader to work out the general technique.

We first note that $89 \equiv -2 \pmod{91}$. Thus we compute $2^{31} \pmod{91}$ and then note that, since 31 is odd, $89^{31} \pmod{91} = -[2^{31} \pmod{91}]$. In order to evaluate $2^{31} \pmod{91}$, we first express the exponent, i.e. 31, in its binary form: $31 = 11111$. The calculation is then as follows:

$$\begin{aligned}2^{31} &\equiv ([(2^2)2]^2 2^2 2)^2 2 \pmod{91}\\ &\equiv [(8^2)2]^2 2^2 2 \pmod{91}\\ &\equiv [(128)^2 2]^2 2 \pmod{91}\\ &\equiv [(37)^2 2]^2 2 \pmod{91}\\ &\equiv [(1369)2]^2 2 \pmod{91}\\ &\equiv [(4)2]^2 2 \pmod{91}\\ &\equiv 8^2 \times 2 \pmod{91}\\ &\equiv 128 \pmod{91}\\ &\equiv 37 \pmod{91}.\end{aligned}$$

Thus $89^{31} \pmod{91} = -37 \pmod{91} = 54$. It works!

Note that instead of needing 30 multiplications to compute $2^{31} \pmod{91}$ we only needed 8. In general, if this particular method is used, then the number of multiplications needed to compute $m^h \pmod{n}$ is $f+g$, where $f+1$ is the number of bits in the binary expansion of h and $g+1$ is the number of 1s in this expression. So, for instance, to compute $m^{11} \pmod{n}$ would require only 5 multiplications. (Note: $11 = 1011$, so $f = 3$ and $g = 2$.)

Anyone interested in more details of the cryptographic applications of number theory should consult reference 5. It is an excellent book but probably beyond pre-university students. Another reference of general interest is reference 4.

References

1. H. J. Beker and F. C. Piper, *Cipher Systems* (Van Nostrand Reinhold, Princeton, NJ, 1982).
2. D. W. Davies and W. L. Price, *Security for Computer Networks* (Wiley, New York, 1984).
3. W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* IT **22** (1976), pp. 644–645.
4. T. H. Jackson, *From Number Theory to Secret Codes: A Computer Illustrated Text* (Adam Hilger, Bristol, 1987).
5. E. Kranakis, *Primality and Cryptography* (Wiley, New York: Teubner, Leipzig, 1986).
6. R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM* **21** (1978), pp. 120–126.
7. I. Stewart, Factorising large numbers, *Mathematical Spectrum* **20** (1987–88), pp. 74–77.

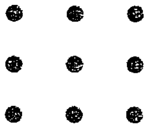
A little bit of geometry

Here are more problems that one of our readers, Arthur Pounder, set at his Maths Club at St. Peter's Grammar School, Prestwich, Manchester. Readers may well have come across them before. If not, why not try them?

Dotty problems

1. Can you arrange nine dots in a plane such that you obtain ten rows with three dots in each row?

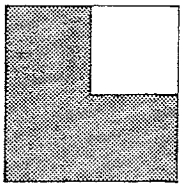
2. Nine dots are arranged in the form of a 3×3 square. Can you join the nine dots together using only four straight lines without taking your pencil off the paper and without retracing any part of a line?



3. In how many ways is it possible to arrange four dots in a plane so that there are only two distinct distances between them?

A nice dissection

4. A square has its upper right-hand quarter removed. Can you dissect the remaining L-shape into four congruent pieces?



A matchstick arrangement

5. Can you arrange six equal matchsticks into four congruent equilateral triangles?

The Jimmy the Greek problem

Devise an uncheatable method for assessing the accuracy of a forecaster who makes probabilistic predictions. Given a history of probabilistic predictions (such as '60% chance of rain today', '70% chance of rain tomorrow') and yes/no outcomes, find a reasonable method for determining how accurate the predictions have been.

MICHAEL A. DE LA MAZA
10 Tumbleweed,
Irvine, CA 92715, USA.

General Meanness

JOHN MACNEILL, *Royal Wolverhampton School*

John MacNeill has taught mathematics at schools in Scotland and is now Head of Mathematics at the Royal Wolverhampton School. He has a long-standing interest in problem-solving and enjoys trying to find new aspects of elementary mathematics, anything more advanced being too great a struggle for his brain.

What does 'mean' mean? Here are some attempts to explain the general idea.

(A) A mean is a measure of central tendency.

(B) A mean is a measure of typicality.

(C) The mean of the scores $x_1, x_2, \ldots, x_n$ is the value μ such that the overall effect would be the same were the n scores all equal to μ.

None of these seems entirely satisfactory. The word 'central' in (A) perhaps begs the question and seems inappropriate for a skewed or bimodal distribution. (B) hardly describes a UK mean of 2.3 children per family. The merits of (C) are that it draws attention to the context and is specific once the effect mentioned is defined.

To illustrate (C), consider three resistances x_1, x_2, x_3 ohms in parallel (figure 1). Here we make the comparison with three equal resistances of μ ohms in parallel. If the effective resistance R ohms is the same in both cases then

$$\frac{1}{R} = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} \quad \text{and} \quad \frac{1}{R} = \frac{1}{\mu} + \frac{1}{\mu} + \frac{1}{\mu},$$

whence

$$\mu = \frac{3}{\dfrac{1}{x_1} + \dfrac{1}{x_2} + \dfrac{1}{x_3}}.$$

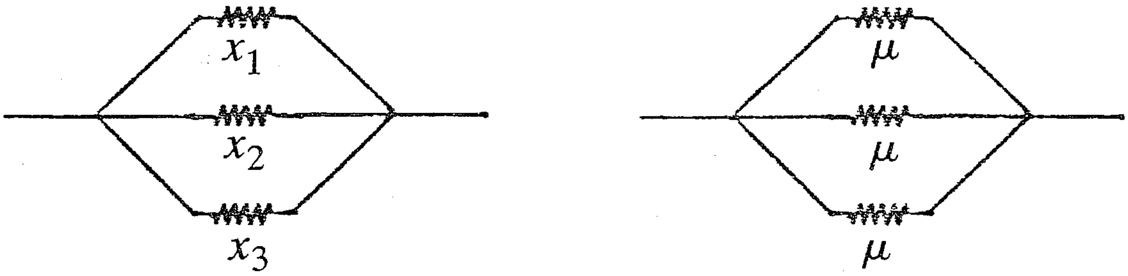


Figure 1

That is, in this context it is appropriate to use the *harmonic mean* of x_1, x_2, x_3. Had the resistances x_1, x_2, x_3 ohms been in series, we would have obtained $\mu = \frac{1}{3}(x_1 + x_2 + x_3)$, the *arithmetic mean* of x_1, x_2, x_3.

Now suppose the height of a magic beanstalk increases by a factor x_1, then by a factor x_2 and then by a factor x_3. Making comparison with the case where the factor is μ each time and the overall increase in height is the same, we find that $\mu = (x_1x_2x_3)^{\frac{1}{3}}$, the *geometric mean* of x_1, x_2, x_3.

Leaving the question of context behind, let us try to see these algebraic formulae for means of different types as special cases of some general formula.

Let

$$(D) \qquad \mu = \frac{x_1g_1 + x_2g_2 + \dots}{g_1 + g_2 + \dots},$$

where $g_1 = g(x_1)$, $g_2 = g(x_2)$, ... for some function $g(x)$ and where $x_1, g_1, x_2, g_2, \dots$ are all positive. If $x_1 = x_2 = \dots = x_n$, then $\mu = x_1$ as (C) would require. Different formulae for μ are obtained by making different choices for $g(x)$. In this way we can find infinitely many varieties of mean; this approach opens up the possibility of establishing results comparing means of various types *via* the functions associated with them.

To illustrate (D), let us consider $n = 2$ and $g(x) = x^r$ for various r; then

$$\mu = \frac{x_1^{r+1} + x_2^{r+1}}{x_1^r + x_2^r}$$

and we have the following.

(1) $r = 0$ gives the arithmetic mean.

(2) $r = -\frac{1}{2}$ gives the geometric mean.

(3) $r = -1$ gives the harmonic mean.

(4) Let μ_t denote the value of μ when $g(x) = x^t$. Then it is not difficult to see that $r > s \Rightarrow \mu_r \geqslant \mu_s$, equality holding only if $x_1 = x_2$.

(5) For two positive numbers,

the arithmetic mean $\geqslant$ the geometric mean $\geqslant$ the harmonic mean,

equality of these means holding only if the two numbers are equal. This result follows immediately from (1), (2), (3) and (4).

Naturally we wish to extend this to apply for $n > 2$. The good news is that (1), (3) and (4) all hold for $n > 2$ and consequently the arithmetic mean is not less than the harmonic mean for $n > 2$. The bad news is that (2) does not hold for $n > 2$ and so although the result of (5) does hold for $n > 2$ we cannot immediately deduce it.

Nonetheless it is possible to accommodate the geometric mean by a generalisation of (D), by permitting g to be a function of n variables: in the expression for μ, $g_1 = g(x_1, x_2, x_3, \dots, x_n)$, $g_2 = g(x_2, x_3, \dots, x_n, x_1)$, $g_3 = g(x_3, x_4, \dots, x_n, x_1, x_2)$ and so on.

As an illustration of this generalisation, the root-mean-square, $\sqrt{\frac{1}{2}(x_1^2+x_2^2)}$, of two positive numbers x_1 and x_2 is associated with the function $g(a,b) = (a-b+\sqrt{2a^2+2b^2})^{\frac{1}{2}}$, as the energetic reader who likes rationalising denominators will wish to prove. It is also of interest to find the root-mean-square of 1 and 7 and also of 7 and 23 both ways: from the definition and *via* g_1 and g_2.

Now for $n = 3$ the geometric mean is associated with the function

$$g(a,b,c) = \frac{b^{\frac{1}{3}}+c^{\frac{1}{3}}}{a^{\frac{1}{3}}}.$$

For then

$$\mu = \frac{x_1^{\frac{2}{3}}x_2^{\frac{1}{3}}+x_1^{\frac{2}{3}}x_3^{\frac{1}{3}}+x_1^{\frac{1}{3}}x_2^{\frac{2}{3}}+x_2^{\frac{2}{3}}x_3^{\frac{1}{3}}+x_1^{\frac{1}{3}}x_3^{\frac{2}{3}}+x_2^{\frac{1}{3}}x_3^{\frac{2}{3}}}{\dfrac{x_2^{\frac{1}{3}}+x_3^{\frac{1}{3}}}{x_1^{\frac{1}{3}}}+\dfrac{x_1^{\frac{1}{3}}+x_3^{\frac{1}{3}}}{x_2^{\frac{1}{3}}}+\dfrac{x_1^{\frac{1}{3}}+x_2^{\frac{1}{3}}}{x_3^{\frac{1}{3}}}}$$

in which the numerator is $x_1^{\frac{1}{3}}x_2^{\frac{1}{3}}x_3^{\frac{1}{3}}$ times as great as the denominator, which becomes clear upon multiplying the denominator by $x_1^{\frac{1}{3}}x_2^{\frac{1}{3}}x_3^{\frac{1}{3}}$. So here $\mu = x_1^{\frac{1}{3}}x_2^{\frac{1}{3}}x_3^{\frac{1}{3}}$ as required.

For $n = 4$ the geometric mean is associated with

$$g(a,b,c,d) = \frac{(b^2c)^{\frac{1}{4}}+(b^2d)^{\frac{1}{4}}+(bc^2)^{\frac{1}{4}}+(c^2d)^{\frac{1}{4}}+(bd^2)^{\frac{1}{4}}+(cd^2)^{\frac{1}{4}}}{a^{\frac{1}{4}}}.$$

In general the geometric mean is associated with the function

$$g(x_1,x_2,\ldots,x_n) = \frac{\sum(x_2^{n-2}x_3^{n-3}x_4^{n-4}\ldots x_{n-1})^{1/n}}{x_1^{1/n}}$$

in which the numerator has $(n-1)!$ terms, none involving x_1.

Despite the complicated appearance of such functions, the following result gives a simple test which often allows comparison of the sizes of different types of mean.

(6) Let $\mu(p)$ and $\mu(q)$ be the means associated with $g = p$ and $g \doteq q$, respectively, in the generalised version of (D), where p and q are suitable functions of n variables. Then $\mu(p) \geqslant \mu(q)$ if $p_jq_k > p_kq_j$ whenever $x_j > x_k$ $(1 \leqslant j \leqslant n,\ 1 \leqslant k \leqslant n)$. If this is so then equality of the means holds only if $x_1 = x_2 = \ldots = x_n$.

An outline of the proof of (6) in the case where $n = 3$ will be enough to convey the idea of the general proof.

For $n = 3$, $\mu(p) \geqslant \mu(q)$

$$\Leftarrow \quad \frac{x_1p_1+x_2p_2+x_3p_3}{p_1+p_2+p_3} \geqslant \frac{x_1q_1+x_2q_2+x_3q_3}{q_1+q_2+q_3}$$

$$\Leftarrow \quad (x_2-x_1)(p_2q_1-p_1q_2)+(x_3-x_1)(p_3q_1-p_1q_3) \\ +(x_3-x_2)(p_3q_2-p_2q_3) \geqslant 0$$

as can readily be verified. This last inequality has three terms on its left side, each of the form $(x_j-x_k)(p_jq_k-p_kq_j)$. In the general case there would be $\frac{1}{2}n(n-1)$ such terms. Since

$$(x_j-x_k)(p_jq_k-p_kq_j) = (x_k-x_j)(p_kq_j-p_jq_k)$$

we may write each such term so that its first factor, x_j-x_k or x_k-x_j, is non-negative. The condition stated in (6) then ensures that its other factor is non-negative. So all terms on the left side are non-negative and the result follows.

To apply (6) it might appear that we have to establish all the implications

$$x_1 > x_2 \Rightarrow p_1q_2 > p_2q_1, \qquad x_1 > x_3 \Rightarrow p_1q_3 > p_3q_1, \qquad \ldots, \\ x_{n-1} > x_n \Rightarrow p_{n-1}q_n > p_nq_{n-1}.$$

Indeed we do, but in cases where, as in this article, the means under consideration are not weighted, that is they are symmetrical in $x_1, x_2, \ldots, x_n$, each function $g(a, b, c, d, \ldots)$ is symmetrical in the $n-1$ variables $b, c, d, \ldots$, and so these implications are all similar algebraically. In such cases it is enough to show that $x_1 > x_2 \Rightarrow p_1q_2 > p_2q_1$. In this way the result of (5) for $n > 2$ can be proved by little more than repeated use of the fact that $x_1^k > x_2^k$ when $x_1 > x_2$ and k is positive.

Thus the scheme outlined here can transfer most of the labour of proving results about means to finding the function associated with each mean, and each such function need be discovered only once. I admit that I know no general procedure for finding these functions, nor have I found a function associated with the root-mean-square of more than two numbers.

Postscript

Since I wrote this article, my attention has been drawn to a paper by Michael E. Mays (see the reference) which deals with various ways of associating means with functions of a single variable for the case $n = 2$. It also contains definitions of 17 means.

Reference

Michael E. Mays, Functions which parametrize means, *American Mathematical Monthly* **90** (1983).

Highly Composite Numbers

ROBERT CANNELL, *University of Manchester*

The author wrote this article whilst studying for a mathematics degree at the University of Manchester.

In the article 'Ramanujan—his life and work' by Ray Hill in Volume 20 Number 1 of *Mathematical Spectrum*, mention is made of Ramanujan's work on highly composite numbers. A *highly composite number* is a positive integer which has more divisors than every smaller positive integer. For example, 2, 4, 6, 12 and 24 are highly composite numbers. Dr Hill mentioned that Ramanujan gave a list of 103 highly composite numbers, the largest one being 6746328388800. I have found a fairly simple way of generating highly composite numbers which makes it possible to find far larger highly composite numbers very quickly.

We first make some simple observations. Consider a positive integer x, and factorize it into its prime factors, say

$$x = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n},$$

where $p_1, p_2, \dots, p_n$ are prime numbers with $p_1 < p_2 < \dots < p_n$. The number of (positive) divisors of x is

$$d(x) = (r_1+1)(r_2+1)\dots(r_n+1),$$

since a typical divisor of x is $p_1^{u_1} p_2^{u_2} \dots p_n^{u_n}$, where $0 \leqslant u_i \leqslant r_i$ for $1 \leqslant i \leqslant n$, and there are r_i+1 possibilities for u_i. Note that we could, if we wished, allow r_i to be zero here. It is clear from this that, for x to be a highly composite number, $p_1, p_2, \dots, p_n$ must be the first n primes, since otherwise we can easily write down a smaller number y with $d(y) = d(x)$. Further, if we permute the powers $r_1, \dots, r_n$, we do not change the number of divisors, so that the smallest number with given powers $r_1, \dots, r_n$ is

$$x = 2^{r_1} 3^{r_2} 5^{r_3} \dots$$

with $r_1 \geqslant r_2 \geqslant r_3 \geqslant \dots$ (where the r_i are zero from some point on). It is clear that every highly composite number must be of this form. The question is: when is such a number highly composite?

Consider such a number x and put

$$\alpha = \min_i p_i^{\{\ln[(r_i+2)/(r_i+1)]\}^{-1}}, \qquad \beta = \max_i p_i^{\{\ln[(r_i+1)/r_i]\}^{-1}},$$

where $p_i^{(\ln 1/0)^{-1}}$ is to mean 1. Note that, even though i ranges over infinitely many values, α and β are both well-defined. We prove that, *if $\alpha \geqslant \beta$, then x is a highly composite number.*

Suppose, on the contrary, that $\alpha \geqslant \beta$, yet x is not a highly composite number. Then there exists

$$x' = 2^{t_1}3^{t_2}5^{t_3}\ldots$$

with $t_1 \geqslant t_2 \geqslant t_3 \geqslant \ldots$, $x' < x$ and $d(x') \geqslant d(x)$. We write $t_i = r_i + s_i$, where s_i may be positive, negative or zero. Now

$$\frac{d(x')}{d(x)} = \prod_i \left(\frac{r_i+s_i+1}{r_i+1}\right).$$

For $s_i > 0$, the binomial expansion gives that

$$\frac{r_i+s_i+1}{r_i+1} = 1+\frac{s_i}{r_i+1} \leqslant \left(1+\frac{1}{r_i+1}\right)^{s_i} = \left(\frac{r_i+2}{r_i+1}\right)^{s_i},$$

so that

$$\begin{aligned}\left(\frac{r_i+s_i+1}{r_i+1}\right)^{\ln\alpha} \leqslant \left(\frac{r_i+2}{r_i+1}\right)^{s_i\ln\alpha} &= \exp\left(s_i\ln\alpha\ln\frac{r_i+2}{r_i+1}\right)\\ &\leqslant \exp(s_i\ln p_i) = p_i^{s_i}.\end{aligned}$$

For $s_i < 0$, we use the inequality

$$\frac{r_i+s_i+1}{r_i+1} \leqslant \left(\frac{r_i+1}{r_i}\right)^{s_i}.$$

This is posed as a problem in the Problems section on page 28. If you cannot prove it, you will have to wait until Volume 21 Number 3 to see a solution! Thus, when $s_i < 0$,

$$\begin{aligned}\left(\frac{r_i+s_i+1}{r_i+1}\right)^{\ln\alpha} \leqslant \left(\frac{r_i+1}{r_i}\right)^{s_i\ln\alpha} \leqslant \left(\frac{r_i+1}{r_i}\right)^{s_i\ln\beta} &= \exp\left(s_i\ln\beta\ln\frac{r_i+1}{r_i}\right)\\ &\leqslant \exp(s_i\ln p_i) = p_i^{s_i}.\end{aligned}$$

Hence, for all i (even when $s_i = 0$),

$$\left(\frac{r_i+s_i+1}{r_i+1}\right)^{\ln\alpha} \leqslant p_i^{s_i},$$

so that

$$\left(\frac{d(x')}{d(x)}\right)^{\ln\alpha} \leqslant p_1^{s_1}p_2^{s_2}p_3^{s_3}\ldots = \frac{x'}{x}.$$

But $\alpha \geqslant 1$ and $d(x')/d(x) \geqslant 1$, yet $x'/x < 1$. There is an obvious contradiction here, so the result is established.

We now illustrate how this result can be used to find a highly composite number x. First choose $r_i = 30$ (say). We wish to choose the other exponents so that

$$p_i^{\{\ln[(r_i+2)/(r_i+1)]\}^{-1}} \geqslant 2^{(\ln\frac{32}{31})^{-1}} \quad \text{for } i > 1.$$

This will ensure that $\alpha = 2^{(\ln\frac{32}{31})^{-1}}$. We also wish to arrange that

$$p_i^{\{\ln[(r_i+1)/r_i]\}^{-1}} \leqslant 2^{(\ln\frac{32}{31})^{-1}} \quad \text{for all } i.$$

This will ensure that $\beta \leqslant \alpha$ and so produce a highly composite number. Note that

$$2^{(\ln\frac{31}{30})^{-1}} \leqslant 2^{(\ln\frac{32}{31})^{-1}},$$

so that what is required is that

$$p_i^{\{\ln[(r_i+1)/r_i]\}^{-1}} \leqslant 2^{(\ln\frac{32}{31})^{-1}} \leqslant p_i^{\{\ln[(r_i+2)/(r_i+1)]\}^{-1}} \quad \text{for } i > 1.$$

Consider $i = 2$, so that $p_i = 3$. A little manipulation will produce the condition

$$\left\{\exp\left(\frac{\ln 3 \ln\frac{32}{31}}{\ln 2}\right) - 1\right\}^{-1} - 1 \leqslant r_2 \leqslant \left\{\exp\left(\frac{\ln 3 \ln\frac{32}{31}}{\ln 2}\right) - 1\right\}^{-1},$$

which gives $r_2 = 19$. If we replace 3 successively by 5, 7, 11 and 13, we obtain $r_3 = 13$, $r_4 = 10$, $r_5 = 8$ and $r_6 = 8$. We note that the primes 11 and 13 occur to the same power, namely 8. The power will stay at 8 until we reach a prime p for which

$$\left\{\exp\left(\frac{\ln p \ln\frac{32}{31}}{\ln 2}\right) - 1\right\}^{-1} < 8$$

or

$$p > \exp\left(\frac{\ln\frac{9}{8}\ln 2}{\ln\frac{32}{31}}\right) = 13.08\ldots.$$

Thus the power of 17 is smaller than 8. In fact, the numbers

$$\exp\left(\frac{\ln\dfrac{r+1}{r}\ln 2}{\ln\frac{32}{31}}\right)$$

give boundaries between the powers of the various primes. If we evaluate these numbers for values of r from 8 to 1 we obtain the boundaries 13.08..., 18.4..., 28.9..., 53.5..., 130.5..., 534.2..., 6990.0... and

3734 030.7.... If we denote by $p(a, b)$ the product of the prime numbers between a and b, this gives the highly composite number

$$x = 2^{30}\times 3^{19}\times 5^{13}\times 7^{10}\times 11^{8}\times 13^{8}\times p(14, 18)^{7}\times p(19, 28)^{6}\times p(29, 53)^{5}\times$$
$$p(54, 130)^{4}\times p(131, 534)^{3}\times p(535, 6990)^{2}\times p(6991, 3734\,031),$$

a vast number well in excess of a million digits! The number of divisors is very approximately $2^{2^{18}}$, a number with about 75 000 digits.

It took me about ten minutes to find this highly composite number with a pocket calculator. Anyone with a home computer and a couple of hours to spare could easily find a highly composite number totally to dwarf even this one.

There does not appear to be an obvious relationship between consecutive highly composite numbers, although with a small one, x say, it is not difficult to find the next such by considering increasing the powers of certain primes and decreasing others to try to obtain the smallest number greater than x which is a highly composite number. Although I have not seen his work, I would guess that this is how Ramanujan found his list of 103 such highly composite numbers, which are presumably consecutive.

There is, however, a connection between the highly composite numbers satisfying the condition given here; let us call them *simple highly composite numbers*. If $x = 2^{r_1}3^{r_2}\ldots p_n^{r_n}\ldots$ is the kth simple highly composite number, we pick out p_i such that

$$p_i^{\{\ln[(r_i+2)/(r_i+1)]\}^{-1}}$$

is minimal. Then $p_i\times x$ is the $(k+1)$th simple highly composite number. This is not difficult to prove.

It is possible to prove that there are fewer than $x^{1/k}$ highly composite numbers less than x for x sufficiently large, but that there are more than $\ln x/\ln 2$. I would tentatively suggest that there are approximately $k\ln x$ highly composite numbers less than x for large x, where k is some constant. Or, more precisely, if $\lambda(x)$ denotes the number of highly composite numbers less than x, then

$$\lim_{x\to\infty}\frac{\lambda(x)}{\ln x}$$

exists and has a positive value (see the Editor's note below). This may be compared with the prime-number theorem, which asserts that, if $\pi(x)$ denotes the number of primes $\leqslant x$, then

$$\lim_{x\to\infty}\frac{\pi(x)}{\dfrac{x}{\ln x}} = 1.$$

Note

In 1944 Paul Erdös proved that there is a constant $c > 0$ (and we can use any $c < \frac{5}{48}$) such that

$$\lambda(x) \geqslant (\ln x)^{1+c} \quad \text{for all large } x.$$

More recently, in 1971, J. L. Nicolas showed that there is a constant b with $\lambda(x) \leqslant (\ln x)^b$ for all large x. Thus

$$1+c \leqslant \frac{\ln \lambda(x)}{\ln \ln x} \leqslant b \quad \text{for all large } x.$$

Assuming that the primes are evenly distributed, Nicolas suggested the conjecture

$$\lim_{x\to\infty} \frac{\ln \lambda(x)}{\ln \ln x} = 1 + \frac{\ln \frac{3}{2} + \ln \frac{5}{4}}{4 \ln 2} = 1.277\ldots.$$

The article by Erdös is in the *Journal of the London Mathematical Society*, Volume 19 (1944), pages 130–133; that by Nicolas is in the *Canadian Mathematical Journal*, Volume 23 (1971), pages 116–130.

Editor

Recovering a number from its cube

Suppose we start with n^3, the cube of a natural number. How can we recover n (apart from using our calculators!)? If n^3 (and so n) is odd, it is quite simple, because then n^3 and n have the same remainder on division by 12. Thus we can divide n^3 by 12 and obtain the remainder r, when n will be r or $12+r$ or $24+r$ etc. For example, start with $n^3 = 50653$. The remainder on division by 12 is 1, so n must be 1 or 13 or 25 or 37 etc. Clearly 1, 13, 25 are no good, and $40^3 = 64000$, so $n = 37$. Not much use, perhaps, but interesting. Can you justify this rule?

The situation is more complicated if n^3 is even, but a similar rule can be developed. Do the same as above, but using 15 instead of 12. If the units digit of n^3 is 0, 4 or 6, this will give n. If the units digit of n^3 is 2, you have to add 6 to the remainder to find n, and if the units digit of n^3 is 8, you have to add 9. All very intriguing! Try it with $n^3 = 175616$, 551368 and 1259712. Again, why does this rule work?

L. B. DUTTA
Maguradanga, Keshabpur
Jessore, Bangladesh.

Collecting

D. J. COLWELL AND J. R. GILLETT, *North Staffordshire Polytechnic*

The authors are lecturers in mathematics at the North Staffordshire Polytechnic. They teach mathematics and statistics to students on engineering and science degree courses.

Introduction

Manufacturers of products such as breakfast cereals often adopt a marketing policy which they hope will appeal to the strong collecting instinct which seems latent in many people. With each item of their product sold they give away some gift, a card say, chosen, presumably at random, from one of a set of different gifts on offer. A serious collector must therefore wonder how many items of the product he must expect to purchase in order to obtain the complete set of N different gifts.

Single purchases

An obvious way to set about building up a collection is to purchase items of the product one by one. Using this approach, if the collection consists at any time of s different gifts $(0 \leqslant s \leqslant N)$, then the expected number of additional items which must be purchased in order to obtain a gift which differs from these s is the mean of a geometric distribution with parameter $(N-s)/N$, namely $N/(N-s)$. Hence the expected number of purchases needed to acquire the full set of N different gifts is

$$\sum_{s=0}^{N-1} \frac{N}{N-s} = N\left(1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{N}\right).$$

The series in this bracket is well known in mathematics and is associated with a constant γ, called *Euler's constant*. This constant has the value $0.5772\ldots$ and is defined as the limiting value as $N \to \infty$ of

$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{N}-\log_e N.$$

Thus the expected number of purchases to obtain a full set, when the purchases are made one by one, may be written, for large N, approximately as

$$N(\log_e N+\gamma).$$

Buying in bulk

Another approach to building up a collection is to buy in bulk in the hope that, with luck, the collection will then contain all or most of the different gifts. Thus, if T items are purchased at one time, we might ask how many different gifts might be expected to be acquired.

To answer this question it is convenient to introduce random variables X_i $(1 \leqslant i \leqslant N)$ which are defined as $X_i = 1$, if the ith gift is acquired, and $X_i = 0$, otherwise. Then

$$P(X_i = 0) = \left(1-\frac{1}{N}\right)^T \quad \text{and} \quad P(X_i = 1) = 1-\left(1-\frac{1}{N}\right)^T.$$

Further,

$$E(X_i) = 1-\left(1-\frac{1}{N}\right)^T.$$

Hence, the expected number of different gifts obtained by a bulk purchase of T items of the product is

$$E\left(\sum_{i=1}^{N} X_i\right) = N\left\{1-\left(1-\frac{1}{N}\right)^T\right\}.$$

Conclusion

For finite values of T, the expected number of different gifts when buying in bulk is clearly less than N. We have also shown that, when collecting by single purchases, we require an average of approximately $N\log_e N + N\gamma$ items to obtain a complete collection.

The latter result suggests that the value of the bulk-buying expected number,

$$N\left\{1-\left(1-\frac{1}{N}\right)^T\right\},$$

should be considered when $T = N\log_e N$.

On writing

$$y = \left(1-\frac{1}{N}\right)^{N\log_e N},$$

we have

$$\begin{aligned}\log_e y &= N\log_e N \log_e\left(1-\frac{1}{N}\right)\\ &= N\log_e N\left(-\frac{1}{N}-\frac{1}{2N^2}-\frac{1}{3N^3}-\dots\right)\\ &= -N\log_e N\left(\frac{1}{N}+\frac{1}{2N^2}+\frac{1}{3N^3}+\dots\right)\\ &< -\log_e N\end{aligned}$$

and thus

$$y < \frac{1}{N}.$$

Hence, by buying $[N \log_e N]+1$ items at one time, we can expect to obtain at least

$$N\left\{1-\left(1-\frac{1}{N}\right)^{[N\log_e N]+1}\right\} > N\left\{1-\left(1-\frac{1}{N}\right)^{N\log_e N}\right\}$$
$$> N\left(1-\frac{1}{N}\right) = N-1$$

different gifts. Since we can obtain at most N different gifts in a bulk purchase, it follows that there is a very high chance that the resulting collection will contain all the N different gifts.

A Graphical Interpretation of the Romberg Integration Process

TONY CROFT, *Crewe and Alsager College of Higher Education*

Tony Croft, a graduate of Leeds University, is a lecturer in mathematics. His research interests are in mathematical modelling, and extrapolation techniques in numerical analysis.

I was prompted by the letter from J. L. G. Pinhey (*Mathematical Spectrum*, Vol. 19 No. 2) to write concerning an illuminating graphical interpretation of the Romberg integration process—one which provides a concrete picture to hold in mind and which stimulates intuition. The background is as follows. In order to approximate an integral

$$I = \int_a^b y \, dx,$$

successive estimates are generated by the trapezium rule which are denoted by T_n, where n denotes the number of strips of width $h = (b-a)/n$ into which the range of integration is divided. It can be shown that the difference between the estimate and the exact answer, i.e. the error, is given by

$$T_n - I = Ah^2 + Bh^4 + Ch^6 + \dots, \qquad (1)$$

where $A, B, C, \dots$ are constants for particular y, a and b. As Pinhey states, the constant A can be eliminated from (1) when T_n and T_{2n} have been evaluated, to obtain an estimate of I, if we ignore terms of order h^4.

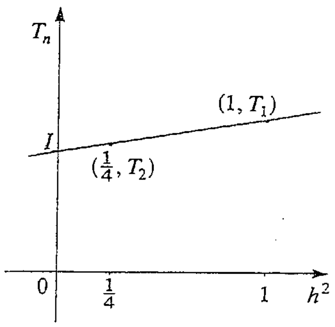


Figure 1

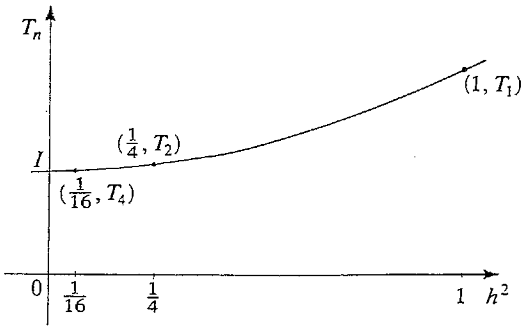


Figure 2

I shall now describe what seems to be a little-appreciated but nevertheless very useful graphical picture of the process. Without loss of generality take $a = 0$ and $b = 1$ so that $h = 1/n$. Taking only the leading term in the error expansion (1), we see that

$$T_n = I + Ah^2,$$

which is of the form $y = mx + c$ with $x = h^2$. The typical graph in figure 1 is obtained by plotting T_n against h^2 using first one and then two strips, i.e. $h = 1$ and $h = \frac{1}{2}$. The straight line joining these two points can then be extrapolated to where $h^2 = 0$. Naturally we would expect that a very thin strip ($h \to 0$) would generate an accurate estimate of the integral and so we take the intercept on the T_n axis as being the limiting value of this estimate. We now see Romberg integration for what it really is: polynomial (in this case, linear) extrapolation. Of course, solution of

$$T_1 = I + A, \qquad T_2 = I + \tfrac{1}{4}A$$

for I yields

$$I = \tfrac{1}{3}(4T_2 - T_1),$$

consistent with Pinhey's result.

Taking two terms in the error expansion (1) we have

$$T_n = I + Ah^2 + Bh^4,$$

which is of the form

$$y = ax^2 + bx + c \qquad \text{with } x = h^2.$$

The typical graph in figure 2 is obtained by taking one, two and then four strips (i.e. $h = 1$, $\frac{1}{2}$ and $\frac{1}{4}$) and plotting the calculated trapezoidal estimates against h^2. A suitable curve fitted through these three points is now a quadratic polynomial and once again we require the intercept on the y axis, since this point corresponds to a strip of width zero. In other words, elimination of both constants A and B in Romberg integration is really quadratic polynomial extrapolation. The process can of course be generalised using higher-degree polynomials when more and more strips are used.

Finally it is worth pointing out that the constants $A, B, \ldots$ in (1) depend upon the derivatives of y. If these fail to exist we would not expect the process to work; for example, with the integral

$$\int_0^1 \sqrt{x}\, dx.$$

Here, the integrand is not differentiable at $x = 0$.

Computer Column

MIKE PIFF

Fourier series

Following on from the Computer Column of Volume 20, Number 1, pages 20 and 21, we investigate the calculation of the Fourier polynomial of an arbitrary periodic function in the following BBC B+ BASIC program.

The program prompts at line 60 for the specification of a function, which must make sense for $-\pi \leqslant X \leqslant \pi$. If return is pressed, the default function is `SIN(X)*INT(X)`. A number must then be input (default 6) for how many cosines and sines are to be included in the Fourier polynomial. After this, the periodic extension of your function is plotted for $-2\pi \leqslant X \leqslant 2\pi$ and then, after a pause, the Fourier polynomial is plotted to the same scale. Press the space bar and the Fourier coefficients are listed out. The mathematics of all this is that if

$$a_0 = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\, dx, \quad a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos nx\, dx, \quad b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin nx\, dx,$$

for $1 \leqslant n \leqslant N$, then

$$g(x) = \tfrac{1}{2}a_0 + \sum_{n=1}^{N} (a_n \cos nx + b_n \sin nx)$$

gives a good approximation to $f(x)$ for large N provided $f(x)$ is suitably well behaved.

Try the functions `X`, `SGN(X)`, `INT(X*X)` and `X*INT(X)` for starters, then try inventing your own spiky functions.

Unfortunately, the BBC computer is very slow on this sort of calculation, so be prepared to wait about a minute for $N = 10$. Fast BASIC on the Atari ST will give a result in about N seconds, for comparison. No doubt the Archimedes could equal this figure.

```
  10 REM Fourier Series Demo
  20 REM M J Piff
  30 *SHADOW
  40 MODE1
  50 f$="SIN(X)*INT(X)"
  60INPUT "Input function of X";f1$
  70IF f1$<>"" THEN f$=f1$
  80nrfterms%=6
  90INPUT "Number of terms";n$
 100IF n$<>"" THEN nrfterms%=VAL(n$)
 110SW=320:SH=256
 120DIM f(SW),g(SW),a(nrfterms%)
 130DIM b(nrfterms%),c(SW),s(SW)
 140OX%=SW DIV 2:OY%=SH DIV 2
 150scale=SW/(4*PI)
 160PROCClearScreen
 170PROCCalcf
 180PROCPlotf
 190PROCCalcg
 200PROCPlotg
 210PROCWait
 220END
 230 REM
 240DEF PROCClearScreen
 250CLG
 260GCOL 0,3
 270MOVE 0,512
 280PLOT 5,1279,512
 290MOVE 640,0
 300PLOT 5,640,1023
 310ENDPROC
 320 REM
 330DEF PROCCalcf
 340LOCAL x%,X,lowx%,highx%
 350LOCAL offset%,step
 360vscale=2^20
 370offset%=SW DIV 2
 380highx%=3*SW DIV 4-1:lowx%=SW DIV 4
 390 step=1/scale
 400 X=-PI-step
 410FOR x%=lowx%TO highx%
 420   X=X+step
 430   f(x%)=EVAL(f$)
 440   vscale=2*vscale
 450   REPEAT
 460     vscale=vscale/2
 470   UNTIL ABS(f(x%)*vscale)<450
 480NEXT x%
 490FOR x%=0 TO lowx%-1
 500   f(x%)=f(x%+offset%)
 510NEXT x%
 520FOR x%=highx%+1 TO SW
 530   f(x%)=f(x%-offset%)
 540NEXT x%
 550ENDPROC
 560 REM
 570DEF PROCCalcg
 580LOCAL x%,lowx%,highx%,i%,ix,ps
 590LOCAL offset%,cx,sx,cix,six,cix1
 600LOCAL step,cx1
 610 ps=PI*scale
 620highx%=3*SW DIV 4-1:lowx%=SW DIV 4
 630 ps=1.0/ps
 640FOR i%=0 TO nrfterms%
 650   a(i%)=0:b(i%)=0
```

```
 660NEXT i%
 670 step=1/scale
 680 cstep=COS(step):sstep=SIN(step)
 690 cx=cstep:sx=-sstep
 700FOR x%=lowx% TO highx%
 710   cx1=cx*cstep-sx*sstep
 720   sx=sx*cstep+cx*sstep:cx=cx1
 730   c(x%)=cx:s(x%)=sx
 740   cix=1:six=0:a(0)=a(0)+f(x%)
 750   FOR i%=1 TO nrfterms%
 760     cix1=cix*cx-six*sx
 770     six=six*cx+cix*sx:cix=cix1
 780     a(i%)=a(i%)+f(x%)*cix
 790     b(i%)=b(i%)+f(x%)*six
 800   NEXT i%
 810NEXTx%
 820 FOR i%=0 TO nrfterms%
 830    a(i%)=a(i%)*ps:b(i%)=b(i%)*ps
 840 NEXT i%
 850FOR x%=lowx% TO highx%
 860   cx=c(x%):sx=s(x%)
 870   cix=1:six=0:g(x%)=a(0)/2
 880   FOR i%=1 TO nrfterms%
 890     cix1=cix*cx-six*sx
 900     six=six*cx+cix*sx:cix=cix1
 910     g(x%)=g(x%)+a(i%)*cix+b(i%)*six
 920   NEXT i%
 930NEXT x%
 940 offset%=SW DIV 2
 950 FOR x%=0 TO lowx%-1
 960    g(x%)=g(x%+offset%)
 970 NEXT x%
 980 FOR x%=highx%+1 TO SW
 990    g(x%)=g(x%-offset%)
1000 NEXT x%
1010ENDPROC
1020 REM
1030DEF PROCPlotf
1040LOCAL x%
1050GCOL 0,1
1060MOVE 0,512+f(0)*vscale
1070FOR x%=1 TO SW
1080   PLOT5,4*x%,512+f(x%)*vscale
1090NEXT x%
1100ENDPROC
1110 REM
1120DEF PROCPlotg
1130LOCAL x%
1140GCOL 0,2
1150MOVE 0,512+g(0)*vscale
1160FOR x%=1 TO SW
1170   PLOT 5,4*x%,512+g(x%)*vscale
1180NEXT x%
1190ENDPROC
1200 REM
1210DEF PROCWait
1220LOCAL t,i%
1230t=GET:CLS
1240 FOR i%=0 TO nrfterms%
1250    PRINT "a(";i%;")=";a(i%),"b(";i%
;")=";b(i%)
1260 NEXT i%
1270ENDPROC
```

Letters to the Editor

Dear Editor,

Subject index

I have prepared a subject index for *Mathematical Spectrum*. I have this on computer disc in 'InterWord' and find it helpful in enabling me to track down articles to enhance any particular topic I am teaching. This is designed for personal rather than commercial use. However, one or two colleagues have suggested that other readers may be interested in it for their own use, and I should be happy to make copies of the disc for a small donation to cover postage and packing.

Yours sincerely,
GREG ATTWOOD
6 Brook End,
Repton, Derbyshire
DE6 6FW.

Dear Editor,

The Knight's Tour

In *Mathematical Spectrum* Volume 19 Number 3, B. R. Stonebridge describes a simple computer program for finding a knight's tour on a chessboard using Warnsdorff's rule. In the last part he generalises this method to higher dimensions and reports on his unsuccessful trials. In fact, a knight's tour in three dimensions is impossible for the triples $(1,2,3)$, $(1,1,2)$, $(1,1,3)$ and $(1,3,3)$.

Proof. The 512 unit cubes have the coordinates $(1,1,1),\ldots,(8,8,8)$ in the usual manner.

(*a*) The triples $(1,2,3)$ and $(1,1,2)$ produce no tour because the sum of the three coordinates is always an odd or always an even integer. (Or, if you colour the cube 'chessboard-wise', you always land on cubes of the same colour.) This means that the tour ends, at the latest, with move number 256.

(*b*) The triples $(1,1,3)$ and $(1,3,3)$ fail because all coordinates change their parity after every move. (For example, if you start on (even, even, even) you land on (odd, odd, odd) and vice versa.) This means that the tour ends at the latest with move number 128.

The triples $(0,1,2)$, $(1,2,2)$, $(0,2,3)$ and $(0,1,4)$ produced, with a LEVEL2 program, a knight's tour for nearly all chosen starting points. Only the triple $(2,2,3)$ failed. I think that a LEVEL3 program would succeed in finding a tour. Maybe an $8\times8\times8$ cube is too small.

Yours sincerely,
HANS ENGELHAUPT
(Franz-Ludwig-Gymnasium,
Bamberg,
W. Germany.)

Dear Editor,

The 1988 puzzle

In attempting to solve this problem (see Volume 20 Number 2, page 53), I found that there are eight numbers which remain obstinate.

I wrote a program to solve the problem to see if the computer could do better. The program used every possible combination of operations given in the problem and took into account factorials up to 19. Double factorials and double square roots were also included. This program came to the same conclusion, i.e. that 42, 50, 51, 52, 53, 75, 77 and 100 cannot be generated, given the rules in the puzzle. There is just one remote possibility: that somewhere there is a difference of two factorials such that the $2n$th root can be taken which gives one or more of the remaining eight numbers or that some factorial plus or minus a function of the remaining digits is a perfect square. I doubt it, however, having investigated some of the possibilities within the power of my computer.

I have generalised the program and can give all the possible results for each year from 0000 to 9999; even the year 2000 is not so barren as it might first seem. If you allow the summation sign, $\sum$, most of the numbers from 1 to 100 can be produced for 2000. I have only tried this by hand, not using the computer, and long strings of numbers in the range 1 to 100 can be produced.

Yours sincerely,
K. M. WILLIAMS
314 Chester Road,
Streetly,
Sutton Coldfield B74 3ED.

Dear Editor,

Pascal's semi-infinite plane

With reference to the article in Volume 20 Number 2 of *Mathematical Spectrum*, it does not seem to be generally well known that Pascal's triangle can be extended to give

$$\binom{n}{r},$$

the coefficient of x^r in the expansion of $(1+x)^n$, when n is a negative integer.

Setting

$$(1+x)^n = \binom{n}{0}+\binom{n}{1}x+\binom{n}{2}x^2+\ldots+\binom{n}{r}x^r+\ldots \quad \text{for } n = 0,-1,-2,\ldots,$$

then, since $(1+x)^0 = 1$, we have

$$\binom{0}{0} = 1, \quad \binom{0}{r} = 0 \quad \text{for } r = 1,2,\ldots.$$

Now, $(1+x)^{n+1} = (1+x)(1+x)^n$ for $n = -1,-2,\ldots,$ so that equating constants and coefficients of x^{r+1} gives

$$\binom{n+1}{0} = \binom{n}{0}, \quad \binom{n+1}{r+1} = \binom{n}{r+1}+\binom{n}{r} \quad \text{for } r = 0,1,2,\ldots.$$

The first result shows that

$$\binom{n}{0} = 1 \quad \text{for all the non-positive integers}$$

and the second result can be rewritten

$$\binom{n}{r+1} = \binom{n+1}{r+1} - \binom{n}{r}. \tag{1}$$

Putting $n = -1$ and $r = 0, 1, 2, \ldots$ gives the binomial coefficients in row -1. Similarly elements in rows $-2, -3, \ldots$ may then be found in turn using equation (1) and the results displayed as shown.

row																	
−7															1		
−6														1		−6	
−5													1		−5		15
−4												1		−4		10	
−3											1		−3		6		−10
−2										1		−2		3		−4	
−1									1		−1		1		−1		1
0								1		0		0		0		0	
1							1		1		0		0		0		0
2						1		2		1		0		0		0	
3					1		3		3		1		0		0		0
4				1		4		6		4		1		0		0	
5			1		5		10		10		5		1		0		0
6		1		6		15		20		15		6		1		0	
7	1		7		21		35		35		21		7		1		0

We can complete the semi-infinite plane in a consistent way by noting that

$$\binom{n}{r} = 0 \quad \text{for } r > n, \text{ where } n = 1, 2, 3, \ldots .$$

Yours sincerely,
R. F. TALBOT
North Staffordshire Polytechnic,
Beaconside, Stafford ST18 0AD.

Dear Editor,

Pythagorean triangles and $\sqrt{2}$

I should like to describe a method of approximating $\sqrt{2}$ which uses Pythagorean triplets. Positive integers x, y, z are said to form such a triplet if $x^2 + y^2 = z^2$, and this triplet is said to be 'primitive' if x, y and z have highest common factor 1. For such a triplet, one of x and y must be even and the other odd. The following formulae describe all primitive Pythagorean triplets with y even:

$$x = p^2-q^2, \qquad y = 2pq, \qquad z = p^2+q^2,$$

where p and q are coprime integers with $p > q > 0$ and one of p and q is even and the other odd. (For example, $p = 2$ and $q = 1$ give the triplet 3, 4, 5.) It is clear that these formulae do give Pythagorean triplets, because

$$(p^2-q^2)^2+(2pq)^2 = p^4+2p^2q^2+q^4 = (p^2+q^2)^2.$$

A right-angled triangle whose opposite and adjacent sides have equal lengths a (say) has its hypotenuse of length $a\sqrt{2}$. Thus if we choose p and q so that x and y are almost equal, we shall obtain an approximation for $\sqrt{2}$ from the formula

$$\sqrt{2} = \frac{2a\sqrt{2}}{a+a} \simeq \frac{2z}{x+y}.$$

In terms of p and q, this gives

$$\sqrt{2} \simeq \frac{2(p^2+q^2)}{p^2-q^2+2pq}.$$

Using a BBC microcomputer, the best values which I have obtained are $p = 33\,461$ and $q = 13\,860$, which give

$$x = 927\,538\,921, \qquad y = 927\,538\,920, \qquad z = 1311\,738\,121,$$

and

$$\sqrt{2} \simeq 1.414\,213\,562,$$

correct to 9 decimal places. I leave it to readers with access to more powerful computers to obtain even better approximations.

Yours sincerely,
PAUL DE SA
Sixth Form
Newcastle Royal Grammar School
Eskdale Terrace, Jesmond,
Newcastle upon Tyne NE2 4DX.

Dear Editor,

The calculation of π

I was fascinated by Keith Devlin's article on π in Volume 20 Number 2. Readers may be interested to know that π has now been calculated to 10^8 places of decimals using iterations described in the article 'Ramanujan and Pi' in *Scientific American* (February 1988), which is more than the 2.9×10^7 decimal places found by NASA's CRAY, mentioned in Keith Devlin's article.

Yours sincerely,
AMITES SARKAR
Sixth Form, Winchester College.

Dear Editor,

Divisibility by 7

In Volume 20 Number 1 page 22 of *Mathematical Spectrum*, L. B. Dutta gave a test for a number to be divisible by 7. Remove its unit digit and subtract twice this digit from the remaining number (for example, 64372 gives $6437-4 = 6433$). Repeat until a single digit remains. (Any resulting minus signs can be ignored.) If the number you end up with is 0 or 7, then the original number is divisible by 7, otherwise not. This test is attributed to a Russian, A. Zbikovski, in about 1861. Readers may like to consider why it works. This method does not tell you anything directly about the remainder when the number is not divisible by 7.

A test which always gives the correct remainder is the following. Multiply the digits of the given number from right to left by the numbers 1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, etc., and add these products, reducing modulo 7 as you go. The final result is the required remainder. For example, from 1234567 we obtain

$$1\times7+3\times6+2\times5+6\times4+4\times3+5\times2+1\times1 \equiv 5 \pmod 7,$$

so the remainder when 1234567 is divided by 7 is 5. A clue as to why this works is that the numbers 1, 3, 2, 6, 4, 5, ... are the remainders when successive powers of 10 are divided by 7.

Yours sincerely,
EDDIE KENT
20 Statham Grove,
Stoke Newington,
London N16 9DP.

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. When writing to the Editorial Office, please state your full name and also the postal address of your school, college or university.

Problems

21.1. (Submitted by Robert Cannell, University of Manchester)
Prove that, for every positive real number r and negative integer s,

$$\frac{r+s+1}{r+1} \leqslant \left(\frac{r+1}{r}\right)^s.$$

(This is used in Robert Cannell's article in this issue.)

21.2. (Submitted by Robert Cannell)
Show that there is a positive integer N such that $x!$ is not a highly composite number when x is an integer greater than N. (See Robert Cannell's article.)

21.3 (Submitted by L. A. Fearnehough, John Ruskin High School, Croydon) Denote by $P_n(x)$ the polynomial $x^{n+1}+(n-x)(x+1)^n$, where n is a positive integer. Prove that

(i) when n is odd, $P_n(x) > 0$ for all real numbers x;

(ii) when n is even, $P_n(x)$ has exactly one real root.

21.4 (Submitted by Russell Baker, University of Sheffield) Determine the number of sequences of n terms using 0, 1 and 2 such that there are no two consecutive 1's and no two consecutive 2's.

Solutions to Problems in Volume 20 Number 2

20.5 When does the polynomial $f(x) = ax^2+bx+c$, with a, b and c real numbers and $a > 0$, have at least one root strictly between 0 and 1?

Solution. Seung Jin Bang, who submitted the problem, describes the possibilities as shown in figure 1. The first two cases are given by $f(0)f(1) < 0$, i.e. $c(a+b+c) < 0$. The third case is given by $c > 0$, $a+b+c > 0$, $b^2-4ac \geqslant 0$.

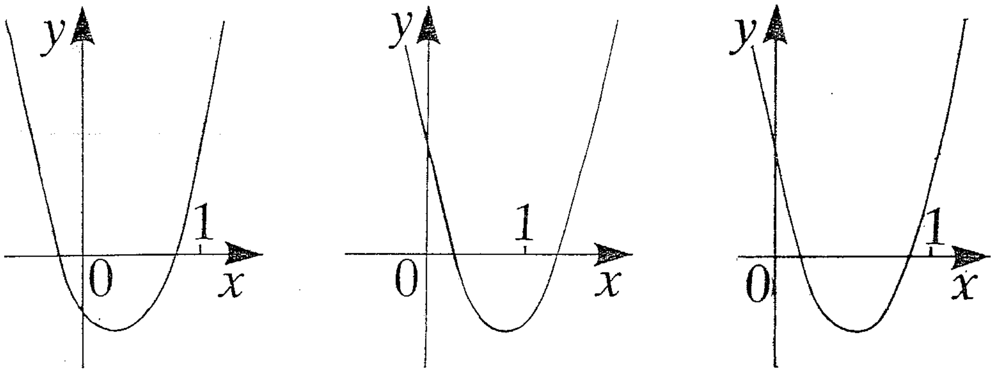


Figure 1

Gregory Economides described this solution by saying that the point $(c/a, b/a)$ must lie in the shaded region of figure 2. All boundaries of the region are excluded with the exception of that formed by the parabola (but not including the points $(0,0)$ and $(1,-2)$).

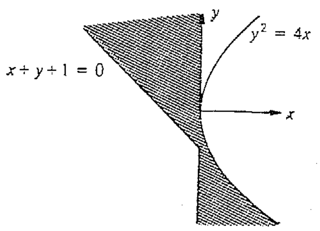
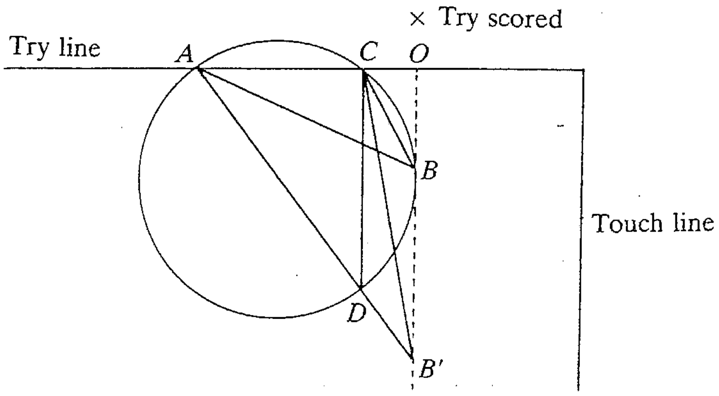


Figure 2

20.6. In the sport of rugby, when a try has been scored a conversion is attempted by a goal-kicker who must score by kicking the ball over a bar between two goal posts. Before attempting the conversion, the kicker must place the ball at any point in a line parallel to the touchline passing through the point where the try was touched down, i.e. the ball must be placed somewhere along the dotted line shown in the figure. Given that a try has been scored outside the goal posts, where should the kicker place the ball?

Solution by Gregory Economides (Royal Grammar School, Newcastle upon Tyne)



Let the points A and C represent the feet of the goal posts and B the point where the ball is placed. If we do not take into account the speed of projection necessary to clear the cross-bar, then the problem reduces to that of locating the point B on the dotted line so as to maximise the angle ABC. Consider the circle passing through the points A and C and tangential to the dotted line. We show that the ball must be placed at the point of tangency. Let B' be any other point on the dotted line and D the point of intersection of the line segment AB' and the circle. Then

$$\angle ABC = \angle ADC = \angle AB'C + \angle B'CD > \angle AB'C.$$

Hence the angle ABC is maximised when the ball is placed at the point of tangency B.

An alternative approach is to use calculus. Put $AO = a$, $CO = b$, $BO = x$, $\angle ABC = \theta$, $\angle ABO = \alpha$ and $\angle CBO = \beta$. Then $\tan\alpha = a/x$, $\tan\beta = b/x$ and $\theta = \alpha - \beta$, so that

$$\begin{aligned}\tan\theta = \tan(\alpha-\beta) &= \frac{\tan\alpha - \tan\beta}{1+\tan\alpha\tan\beta} \\ &= \frac{(a-b)x}{x^2+ab}.\end{aligned}$$

Thus

$$\sec^2\theta\,\frac{\mathrm{d}\theta}{\mathrm{d}x} = \frac{(x^2+ab)-2x^2}{(x^2+ab)^2}(a-b),$$

and this is zero when $x^2 = ab$. This clearly gives a maximum value of θ. Thus the ball should be placed a distance from O along the dotted line which is the geometric mean of its distances along the try line from the feet of the goal posts. These two answers are the same.

20.7. Denote by $C(n,k)$ the list of natural numbers which can be written in binary form using k 1's and $n-k$ 0's, arranged in increasing order. In $C(14,8)$, where does 10101110101001 occur in the list, and what is the 19 187th term in $C(19,11)$?

Solution by Gregory Economides

Written in binary form, the first term in $C(n,k)$ is 10...01...1, i.e. 1 followed by $n-k$ 0's followed by $(k-1)$ 1's, and

$$1\ \underbrace{0\ldots0}_{n-k-r}\ 1\ \underbrace{0\ldots0}_{r}\ \underbrace{1\ldots1}_{k-2}$$

is the $\left[\binom{r+k-2}{k-1}+1\right]$th term for $1 \leqslant r \leqslant n-k$, where $\binom{r+k-2}{k-1}$ denotes the binomial coefficient. Hence 10101110101001 is the

$$\left\{\binom{11}{7}+\binom{9}{6}+\binom{8}{5}+\binom{7}{4}+\binom{5}{3}+\binom{3}{2}+1\right\}\text{th}$$

term in $C(14,8)$, i.e. the 519th. Also,

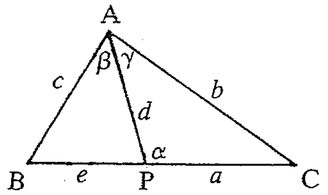
$$19\,187 = \binom{16}{10}+\binom{15}{9}+\binom{14}{8}+\binom{13}{7}+\binom{12}{6}+\binom{11}{5}+\binom{7}{4}+\binom{6}{3}+\binom{5}{2}+\binom{4}{1},$$

so that the 19 187th term in $C(19,11)$ is, in binary form, 1011111100011110000, or 391 408 to base 10.

Of course different answers will be obtained if you allow strings to begin with 0.

20.8. Let P be a point on side BC of triangle ABC. If $(\mathrm{AP})^2 = (\mathrm{AB})(\mathrm{AC})-(\mathrm{PB})(\mathrm{PC})$, prove that either AB = AC or that AP bisects angle BAC.

Solution by Amites Sarkar (Winchester College)



With the labelling shown in the figure, the cosine rule gives

$$b^2 = a^2+d^2-2ad\cos\alpha, \qquad c^2 = e^2+d^2+2ed\cos\alpha,$$

so that, if we eliminate $\cos\alpha$, we obtain

$$eb^2+ac^2 = ea^2+ed^2+ae^2+ad^2.$$

It is given that $d^2 = bc-ae$, so that this simplifies to give

$$eb^2+ac^2 = ebc+abc,$$

or

$$(eb-ac)(b-c) = 0.$$

Thus either $b = c$, i.e. AB = AC, or $eb = ac$. Assume the latter. Then the sine rule gives

$$\frac{a}{\sin\gamma} = \frac{b}{\sin\alpha} = \frac{bc}{c\sin\alpha} = \frac{bc}{c\sin(\pi-\alpha)} = \frac{be}{c\sin\beta} = \frac{a}{\sin\beta},$$

so that $\beta = \gamma$ and AP bisects angle BAC.

Also solved by Gregory Economides, who also proved the converse.

The 1988 puzzle

This appeared on page 53 of Volume 20 Number 2. The aim was to express the numbers 1 to 100 in terms of the digits of the year in order, using only the operations, $+$, $-$, $\times$, $\div$, $\surd$, ! and concatenation (i.e. forming 19 from 1 and 9, for example). Eleven numbers resisted our efforts; readers succeeded with three of these:

$$44 = -1+[(\sqrt{9})!]!\div(8+8), \qquad 46 = 1+[(\sqrt{9})!]!\div(8+8),$$

$$99 = 1+[(\sqrt{9})!]!\div 8+8.$$

This leaves 42, 50, 51, 52, 53, 75, 77 and 100. There were some attractive expressions: for example, $28 = 1\times\sqrt{98}\times\sqrt{8}$ from Sanjay Sanghani of Repton School and $45 = (1+9)!\div(8!+8!)$ from K. M. W. Williams of Streetly. As usual, the 'illegal' expressions were the most amusing: for example, Mr Williams came up with

$$52 = \frac{(\sqrt{9})!}{.1} - \sqrt{8\times 8}$$

and

$$(1+9\sqrt{\ })(8+8) = (8+8)+9\sqrt{8+8} = 52.$$

Reviews

The Pólya Picture Album—Encounters of a Mathematician. Edited by G. L. ALEXANDERSON. Birkhäuser, 1987. Pp. 160. 68 Swiss Francs.

This surely must be the strangest book to arrive for review in our editorial office. It will fascinate the professional mathematicians amongst our readership and perplex all others.

George Pólya was born in Budapest in 1887 and died in 1985. During his very full life, he was a distinguished mathematician, holding professorships in Zürich and latterly at Stanford University in the USA. He travelled extensively, meeting many distinguished mathematicians. And with him went his camera. The present volume is a photographic record of encounters with the famous (mathematically famous, that is). Each photograph is accompanied by a comment from Pólya. My favourite among these accompanies a photograph of David Hilbert (page 47). Pólya tells a story to illustrate Hilbert's absentmindedness: 'He and his wife were giving a party at their home when Mrs. Hilbert noted that he had failed to put on a fresh shirt, so she told him sternly to go upstairs and put on a clean one. But he didn't come back. So after a while she went upstairs and found he was in bed. You see, he did things in their natural sequence. He had gone upstairs, taken off his coat, then his tie, his shirt and so on, and then got into bed.'

Mathematical Spectrum is fortunate to have George Pólya amongst its list of contributors. In Volume 2 Number 1 (1969/70), he wrote on the isoperimetric theorem. The question considered was: of all plane figures having the same perimeter, which one has the largest area?

Throughout his mathematical life, George Pólya was fascinated by mathematical problems. His book *How To Solve It* has sold over one million copies and has been translated into at least 17 other languages, a mathematical best-seller of recent times.

A fascinating glimpse into the men and women (see Emmy Noether on pages 82, 83) who have made mathematics.

University of Sheffield DAVID SHARPE

The History of Mathematics: A Reader. Edited by JOHN FAUVEL and JEREMY GRAY. Macmillan Education in association with The Open University 1987. Pp. xxiv + 628. Hardback £30·00 (ISBN 0 333 42790 4), paperback £9·95 (ISBN 0 333 42791 5).

Three cheers for this delightful new source book on the history of mathematics! This selection of readings is designed for students of the Open University course MA290 *Topics in the History of Mathematics*, but its appeal will be much wider. All serious students of the history of mathematics should welcome this handsome volume on to their bookshelves.

The work's in-depth comprehensive coverage of mathematical developments from ancient times to the present day establishes it as the leader in its field. Many of the over 400 chosen extracts have been translated into English for the first time, and many have never before been anthologized. The book is arranged in a broadly chronological framework, and each chapter is prefaced with a brief introduction. Perhaps the most attractive feature of this treasury is its rich variety of sources, including formal texts, letters, diaries, novels and plays—all combining together to paint a fascinating picture of the role which mathematics has played throughout history.

Many interesting and surprising facts are tucked away in the leaves of this reader. For example, did *you* know that our earliest record of the problem of 'squaring the circle' is to be found in the work of the Athenian comic dramatist Aristophanes? The authors are to be congratulated on compiling this anthology, which succeeds in capturing something of the excitement of these times, when the history of mathematics is a more lively discipline than ever before.

University of Sheffield R. J. WEBSTER

Discovering Mathematics: The Art of Investigation. By A. GARDINER. Clarendon Press, Oxford, 1987. Pp. xiv + 206. Hardback £20 (ISBN 0 19 853282 2), paperback £10 (ISBN 0 19 853265 2).

In pure mathematics we are more interested in the search for answers than in the answers themselves. The situation is similar to that in the film *North by Northwest* where our attention is captured by Cary Grant's exploits crossing America rather than by the secret plans which are the cause of his journey.

The book under review places the emphasis firmly on the search and not on the mathematical results we are searching for; I would have preferred the title 'Searching for Mathematics', 'discovering' does stress the end-result of the search. The book contains four short investigations and two long ones. The reader is led through a series of comments and words of advice, exercises, hints and solutions. As an example, we are led to find which amounts can be made up using only 5-cent and 8-cent stamps.

Tony Gardiner is to be applauded for his choice of both mathematics and exercises. The mathematics is about familiar objects, such as digits and multiplication, so that the readers can step out boldly in their search and need not be hesitant about what they are allowed to do. The exercises avoid the traditional mathematics problem, which is notorious for appearing impossible before we see the answer and easy after, and which gives mathematics its reputation for being difficult. Instead, the exercises offer a sequence of interesting and sensibly challenging tasks.

University of Sheffield A. K. AUSTIN

Alpha Mathematics Handbook. By LENNART RÅDE. Chartwell-Bratt, Old Orchard, Bickley Road, Bickley, Bromley, Kent BR1 2NE, 1987. Pp. 199. Hardback £4·95 (ISBN 0 86238 036 7).

You are sitting in your school or college library, doing mathematics. Now, which is union and which is intersection for sets? Or: what is de Moivre's theorem for complex numbers? Or: what is the volume of a cone? Or: what is $\tan 2x$ in terms of $\tan x$? Or: what BASIC program will tell me whether a number is prime? Or: what is Bayes' formula for conditional probability? Or: what is Avogadro's constant? You can find answers to all these questions and lots more readily available in this handbook. It is a mine of information, all there at a glance.

I particularly enjoyed the pictures and potted biographies of some of the great mathematicians. But I think my favourite inclusion is the devil's curve.

An invaluable addition to any school or college library. And, at such a modest price for a hardback book, a very useful addition to any mathematics student's personal library.

University of Sheffield DAVID SHARPE

A Diary on Information Theory. By ALFRED RÉNYI. John Wiley and Son, New York, 1984. Pp. 125. £16·50.

This book is by an outstanding Hungarian mathematician, and is written in the form of a diary, as though a university student on the subject is writing down his thoughts. The first part consists of chapters labelled 'lectures', and covers a number of ideas on information theory and probability. Then there are chapters on games, teaching of probability theory and the mathematical theory of trees.

I found the book most interesting (and entertaining, for example the quotation 'the main goal of education at university is that professors should teach only what is missing from the text books and exists only in their minds'). Sixth-formers will find the book readable and stimulating, and undergraduates reading information theory will find it enlightening. The price is likely to put it out of the reach of individuals, but libraries should get a copy.

Josiah Mason Sixth Form College, Birmingham PETER FOSTER

Discrete Mathematics and Algebraic Structures. By LARRY J. GERSTEIN. W. H. Freeman and Company, 1987. Pp. 413. Hardback £32·95 (ISBN 0 7167 1804 9).

Tim O'Shea, Professor of Information Technology and Education at the Open University, was recently quoted as saying that a computer scientist who doesn't know modern mathematics is like an engineer who doesn't know what a Fourier transform is. He would have in mind topics such as those introduced in this well-organised book, which should fascinate the mathematician or computer scientist in the making, sixth-former or first-year undergraduate, and which reveals much about the nature of mathematics. Due place is given to rigorous proof, but often with a preamble in conversational style, and the exercises are not needlessly hard. A problem for the reader is the very quantity of concepts, terms and notations to be found in such a wide-ranging book; an index of notation would help.

Other minor grumbles: 'Jones likes waffles if and only if it is not the case that Jones dislikes waffles' (p.29) is false; the term 'theorem' is explained but not 'lemma'. Oh dear, what can lemmata be?

Recommended as a good basis for further study.

The Royal Wolverhampton School JOHN MACNEILL

Principles of Dynamics. By J. GROSJEAN. Stanley Thornes (Publishers) Ltd., 1986. Pp. xiv+288. £7·50.

Many books on dynamics follow the style of Ramsey's *Dynamics* with the material updated. This book, however, is somewhat different and takes a full-blooded engineering approach. It may not be suitable as an A-level text but it has a whole series of practical examples which can be adapted for use in more traditional courses. I particularly liked the section on four-bar linkages with applications to cranes, diggers and airliner nosewheels and the section on particle mechanics. The book is very readable and will stimulate the interest of teachers, who are looking for examples that are a bit different, and of students who are intending to study engineering. I thoroughly recommend the book.

University of Sheffield D. M. BURLEY

Introduction to Discrete Mathematics for Software Engineers. By TIM DENVER. Macmillan, 1986. Pp. ix+309. Hardback £25·00 (ISBN 0 333 40736 9), paperback £12·00 (ISBN 0 333 40737 7).

Software engineering is concerned with the design and implementation of complex computer systems based principally, but not exclusively, on the construction of large programs written in various computer languages—at both high and low levels. The need to make these systems reliable and safe, as well as economically acceptable, is placing a great many pressures on the computing industry; pressures which are forcing a substantial rethink about what the software design process should be. The sort of systems that we are needing to deal with can be extremely large and complex, perhaps involving thousands of man-years of work, and so the sheer scale of the task is something we can hardly bear to contemplate.

The software engineer is well served by this book. It represents a genuine attempt to bridge the gap between the development of mathematical skills needed in this area with the process of putting them into practice. The examples used to motivate concepts are, within reason, typical of many of the application areas of interest to software engineers. Some of these problems are returned to as sources of more advanced examples and this continuity is a good feature of the book. I envisage that it will help to encourage much more use of formal methods in software engineering, and I recommend it strongly.

University of Sheffield MIKE HOLCOMBE

Centres of Gravity. Micros in Mathematics (MIME) Project. John Wiley Software, 1986. Pp. 9+43 workcards+2 BBC Disks. £34·95.

This set of disks is No. 11 in a series of thirteen covering various aspects of mechanics for sixth forms. The rest of the series includes projectile motion, Newton's laws, friction, etc., each unit at the price given above.

Centres of Gravity uses various systems to illustrate the calculation of centroids, such as a system of four particles, or a hemispherical shell, and then demonstrates toppling using a graphics representation of a child's kelly, and a double-decker bus.

I was not impressed with this package. Although the graphics of the bus was neat, it seems to me that the computer demonstrations should at least show something that cannot be done more easily with a physical model. The ideas involved here are so slight that surely the elaborate computer simulation can add little to a student's intuition of what will happen.

My other criticism is on the grounds of value for money. The price seems steep for what is offered. The writing on the workcards rarely extends more than a third of the way down, and little mathematical theory is included.

Not the best package I have seen.

University of Sheffield MIKE PIFF

Introduction to Probability. By D. R. ROBINSON and A. W. BOWMAN. Adam Hilger, 1986. Pp. viii+91+1 BBC Disk. £15·00.

This title is part of an excellent series of computer illustrated texts. The ground covered includes binomial, normal and Poisson distributions; distribution and density functions; expectation and variance; the central limit theorem; and transformations of random variables. The text and instructions for running the programs are clear, and the simulations are well presented and entertaining. A nice touch is the automatic rescaling of any barcharts which threaten to overflow the screen area. A minor criticism is that the programs are menu-driven, but the individual programs do not include an option to return to the main menu; you have to press ⟨shift⟩+⟨break⟩ again.

The package is a fine way to develop the student's intuition about random phenomena, and is good value for money.

University of Sheffield MIKE PIFF

The Best of Teaching Statistics

184 pages of resource material for all levels of statistics teaching. Ideas for use in GCSE mathematics and statistics courses; applications relevant to A-level and the new AS-level syllabuses in statistics.

The 41 best articles from the first five years of *Teaching Statistics* are classified under:

Statistics in the Classroom
Practical and Project Work
Pupil's Understanding
Teaching Particular Topics
Statistics in Society.

Most teachers are likely to find the practical and project work section...a mine of helpful information'

The Statistician

'There is truly something here for everyone interested in teaching statistics'

Statistics Teacher Network'

Price £6.00 (plus 70p post and packing)

Cheques payable to:
Teaching Statistics

Order from: Centre for Statistical Education, Department of Probability and Statistics, University of Sheffield, Sheffield S3 7RH

Why not also subscribe to the journal *Teaching Statistics* on a regular basis? Write to the address above for details.

CONTENTS

ISSN 0025-5653

PRICES (*postage included*)

Prices for Volume 21 (Issues Nos. 1, 2 and 3)

Subscribers in	*Price per volume*	
North, Central and South America	US$11.00 or £6.00	(Note: These overseas prices apply even if the order is placed by an agent in Britain.)
Australia	$A16.00 or £6.00	
Britain, Europe and all other countries	£4.80	

A discount of 10% will be allowed on all orders for five or more copies of Volume 21 sent to the same address.

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, England.

Published by the Applied Probability Trust
Typeset by the University of Nottingham
Printed in England by Galliard (Printers) Ltd, Great Yarmouth