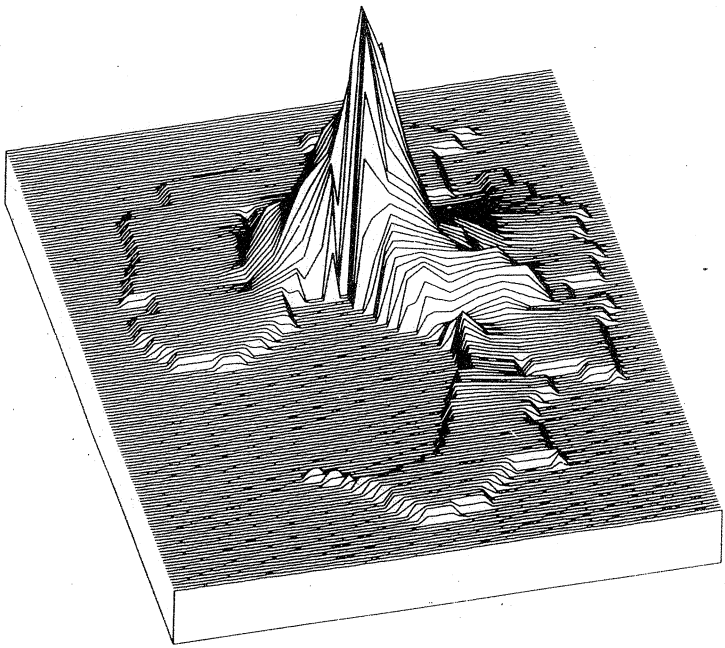
ISSN 0313-6825

Function

Volume 4 Part 5

October 1980



A SCHOOL MATHEMATICS MAGAZINE

Published by Monash University

Function is a mathematics magazine addressed principally to students in the upper forms of schools. Today mathematics is used in most of the sciences, physical, biological and social, in business management, in engineering. There are few human endeavours, from weather prediction to siting of traffic lights, that do not involve mathematics. *Function* contains articles describing some of these uses of mathematics. It also has articles, for entertainment and instruction, about mathematics and its history. Each issue contains problems and solutions are invited.

It is hoped that the student readers of *Function* will contribute material for publication. Articles, ideas, cartoons, comments, criticisms, advice are earnestly sought. Please send to the editors your views about what can be done to make *Function* more interesting for you.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

Articles, correspondence, problems (with or without solutions) and other material for publication are invited. Address them to:

The Editors,
Function,
Department of Mathematics,
Monash University,
Clayton, Victoria, 3168.

Alternatively correspondence may be addressed individually to any of the editors at the addresses shown above.

The magazine will be published five times a year in February, April, June, August, October. Price for five issues (including postage): $4.50; single issues $1.00. Payments should be sent to the business manager at the above address: cheques and money orders should be made payable to Monash University. Enquiries about advertising should be directed to the business manager.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

Registered for posting as a periodical - "Category B"

Our authors in this issue include two mathematicians from overseas. Both have visited Monash University for several months this year. *Hans Kaiser* is a Professor of Mathematics in Vienna. He specializes in algebra, but has recently developed a strong interest in the history of mathematics. His article is in the latter area. *Simon Tavaré* is from the University of Utah, where he teaches mathematical statistics. His research interests include devising and analysing probability models to explain genetic evolution. With the current controversy in the newspapers about evolution, we believe his article will be of especial interest.

THE FRONT COVER

The illustration depicts a computer plotted contour map of estimated daily petrol consumption for Melbourne in 1976. The peak represents a consumption of 30 000 litres of petrol per square kilometre per day in the city, with lesser consumption in the suburbs (and bay!).

The data for the plot was generated by an urban planning computer model called TOPAZ which can evaluate alternative urban forms in terms of economic, energy, pollution, transport and other infrastructure impacts. TOPAZ was developed at CSIRO Division of Building Research, Highett.

We thank Dr Ron Sharpe for permission to use the photo.

CONTENTS

Topics in the History of Statistical Thought and Practice. V. The Introduction of the Numerical Method into Clinical Medicine. P.D. Finch. 2

The Two Faces of Coding Theory. John Stillwell 8

Where Did Conic Sections Come From? H.K. Kaiser 16

Letter to the Editors: The Game "Splat". Ravi Sidhu 24

Mathematical Models in Population Genetics. Simon Tavaré 26

Problem Section (Problems 4.5.1, 4.5.2, 4.5.3; Solutions to problems 4.1.2, 4.2.4, 4.3.2, 4.4.4) 30

TOPICS IN THE HISTORY OF STATISTICAL THOUGHT AND PRACTICE

V. THE INTRODUCTION OF THE NUMERICAL METHOD INTO CLINICAL MEDICINE†

P.D. Finch, Monash University

When we are ill and go to our doctor we expect to be cured. We assume he knows his treatment is likely to be successful and to lack harmful side-effects. That our confidence is not misplaced is largely due, in the first instance, to one man, Pierre-Charles Alexandre Louis (1787-1872). It was Louis who introduced into clinical medicine a systematic procedure of investigation, *viz.* the so-called 'numerical method'. These days we would call it 'statistical analysis'.

But it would be misleading to suggest that Louis' importance rests on what he did with data. His actual analyses are crude and primitive and, not surprisingly, seldom meet current standards of statistical enquiry. It was his insistence on the *need* to collect data which singled him out from his predecessors and contemporaries. Instead of merely theorizing about disease and the therapeutic effects of proposed treatments, he went out and collected evidence. It seems obvious to us nowadays that one needs to study actual cases to determine whether a treatment is, on the whole, effective. But in Louis' day, this was a novel idea. His greatness, like that of most great men of science, is that he was one of those who sees the obvious the rest of us miss. In a talk to the French Academy of Medicine he expressed his viewpoint in the following words:

"The object of medical statistics is the most rigorous determination which is possible of general facts, which, in my opinion, cannot be arrived at without their assistance. Thus a therapeutic agent cannot be employed with any discrimination or probability of success in a given case unless its general efficacy, in analogous cases, has been previously ascertained; therefore I conceive that without the aid of statistics nothing like real medical science is possible."

---

† Text of a schools' lecture delivered on 21st March 1980 at Monash University.

The usefulness of Louis' viewpoint can be illustrated by his work on the efficacy of bloodletting, the then standard treatment in inflammatory diseases. This work appeared in journal articles in 1828 and was published in book form in 1835. It was translated into English in 1836. The following quotation from the preface to that translation, by James Jackson MD, makes it clear that in medicine, at least, Louis' approach was seen as something of a novelty.

"M. Louis has not brought forward a new system of medicine; he has only proposed and pursued a *new method* in prosecuting the study of medicine. This is nothing else than the method of induction, the method of Bacon, so much vaunted and yet so little regarded. But if so where is the novelty? If any one, after patiently studying and practising the method proposed by M. Louis, denies the novelty of it, I will not dispute with him a moment. Perhaps he will then agree with me that it is a novelty to pursue the method of Bacon thoroughly and truly in the study of medicine; though it is not new to talk of it and laud it."

TABLE 1. DURATION (IN DAYS) OF PNEUMONITIS (50 NON-FATAL CASES)

	Day of first bleeding							
1	2	3	4	5	6	7	8	9
10	7	16	12	13	13	12	12	11
12	10	17	12	13	16	15	13	17
14	12	19	12	17	17	18	18	30
		20	15	21	23	19	19	35
		20	16	28	35	24	20	
		29	19	40		27	21	
			21					
			22					
			25					
			28					
			40					
Mean duration 12	10	20	20	22	21	19	17	23

TABLE 2. DAYS TILL DEATH FROM PNEUMONITIS (27 FATAL CASES) AND AGE (IN BRACKETS)

Day of first bleeding

1	2	3	4	5	6	7	8	9
6(18)	8(65)	4(57)	12(85)	8(63)	10(40)	20(68)	25(40)	22(50)
	12(55)	6(30)	15(37)	9(24)	29(24)			
	12(69)	6(47)	17(67)	16(58)	62(20)			
	17(75)	11(45)	20(22)					
	53(65)	16(54)	29(19)					
		47(75)	29(46)					
			Mean duration					
6	20	15	20	11	33	20	25	22

Blood-letting fell into disuse largely because Louis was able to show that its benefits were not so great as was commonly supposed. Some extracts from his data are given in Tables 1 and 2. These refer to 77 cases of pneumonitis all of whom were in perfect health when symptoms first developed. Of these cases, 50 recovered after blood-letting and 27 died. The data portrays the relationship between length of disease and day of first bleeding. For the fatal cases, age is also recorded. If blood-letting were effective, then one might anticipate that early treatment would shorten the duration of disease. Louis noted that in Table 1 this did seem to be the case for blood-letting in the first two days, whereas after that it seemed to make "but little difference whether it was commenced a little sooner or a little later". Nevertheless there is almost as much variability in duration of disease within the later columns as there is between them and the first two columns and, as Louis said, "differences no less considerable... would have unquestionably have existed among the cases bled within the first twenty-four or forty-eight hours, if their number had been greater...". He noted too that there was no appreciable age difference between those bled early and those bled late, the average ages of those bled for the first time before and after the fourth day being 33 and 36 years respectively. Louis also insisted that, in all these cases, the "violence of the disease" was the same and the treatment "equally energetic". He concluded: "the utility of bleeding has been very limited in the cases thus far analysed". He found further limitations when he considered the 27 fatal cases. Of these, he noted, 18 were bled within the first four days and there seemed some slight association between early bleeding and early death although, as Louis pointed out, this may be partly an age effect because those bled early tended, on the whole, to be the older patients.

Extracts from Louis' book are given in the Penguin History of Medicine edited by King (1971). As we said before, the importance of his contribution to medicine was the method he introduced rather than the specific results he obtained. He argued that no two cases are exactly the same and that it is

precisely on this account that enumeration is necessary to compensate for the differences between them when a number of treatments are being compared. "By doing so", he said, "the errors (which are inevitable), being the same in two groups of patients subjected to different treatment, mutually compensate each other, and they may be disregarded without sensibly affecting the exactness of the results."

Louis influenced many students who went to study medicine in Paris. They came from the U.S.A., England and other parts of Europe. One of his students was Oliver Wendell Holmes (1809-1894), the eminent American man of letters who had graduated from the Harvard Medical School in 1836. In 1843 Holmes published a literature survey suggesting that puerperal or child-bed fever was communicated to the obstetrical patient by the physician. This was an unpopular view among medical men at that time. But his study did not measure up to the 'numerical method' and though sounder work was done independently by Ignaz Semmelweiss (1818-1865), a pupil of Josef Skoda (1800-1881) who was himself a pupil of Louis, it was not until more was known about bacteria that the medical profession was finally convinced.

Among Louis' English students was William Guy (1810-1885). He returned from Paris and became a professor, first of Forensic Medicine and then of Hygiene. He was an early member of the London (now Royal) Statistical Society which was founded in 1834, and he eventually became its president. He was an influential exponent of Louis' ideas; for example, in 1839 he emphasized that "where identity ceases, there certainty ends, and probability begins; and there too the numerical method finds its first application". (This quotation comes from Guy's article listed in the references at the end.) In England, however, the most important disciple of Louis was William Farr (1807-1883) who was appointed the Compiler of Abstracts to the General Register Office in 1839, a position he held for over 40 years. It was Farr who supplied much of the data Snow used in his study of the communication of cholera (*Function* Volume 3, Part 1, pp. 22-27). Among the people he influenced were Florence Nightingale (1820-1910) who was one of the founders of the Royal Statistical Society, and Francis Galton (1822-1911), a cousin of Charles Darwin and one of the founders of genetics.

As Louis' ideas became more widely known it became apparent that many issues in public health could be clarified by the examination of appropriate data. Causes of disease and the death rate were matters of concern at that time, as Farr said: "The death rate is a fact; anything beyond this is an inference." Gradually the *quantitative* patterns of disease and death were painstakingly uncovered. For example, the death rate was clearly exposed as related to social class. Table 3 illustrates this in an unmistakable manner: about two-thirds of the working class died before age 20 whereas about three-quarters of the 'gentry' survived to that age. The clear statement of such facts by means of the numerical method played a key role in the movement for social reform.

TABLE 3. LIFE TABLE FOR BOROUGH OF PRESTON, ENGLAND, BY SOCIAL CLASS, 1843

	Percentage still alive		
End of Year	Gentry	Tradesmen	Workers
1	91	80	68
5	82	62	45
10	81	57	39
20	76	52	32
30	72	46	25
40	63	38	20
50	56	28	16
60	45	21	11
70	25	13	6
80	8	5	2
90	1	0.8	0.2

For every 100 males born, the table shows the number who would still be alive at various later years.

Again, the collection of appropriate data put beyond doubt the efficacy of smallpox vaccination. This is illustrated in Table 4.

TABLE 4. SURVEY OF CHILDREN IN SMALLPOX EPIDEMIC LONDON, 1863

Vaccinated	Number	Smallpox	Rate per 1000
Yes	49 570	88	1.78
No	2837	1010	356

Moreover, once such issues had been decided, the medical profession could then turn to more sophisticated questions. For instance, did the degree of protection depend on the degree of vaccination? Table 5 is an example of the results of such an enquiry. Again the thrust of the answer is unmistakeable. The more treatments a patient had with the vaccine, the lower his chance of catching smallpox.

TABLE 5. SMALLPOX INCIDENCE BY DEGREE OF VACCINATION, LONDON, 1863

Number of Vaccine Treatments	Rate per 1000 of smallpox
1	6.80
2	2.49
3	1.42
4+	0.67

Increasingly throughout the 19th century, various diseases were studied by the numerical method. A new subject gradually arose from these modest beginnings; today we call it epidemiology. Substantially the same methods are still in use today. To illustrate this, Table 6 gives some data collected by the Center for Disease Control (CDC) in the U.S.A. to see if laws requiring immunization for measles were effective.

TABLE 6. MEASLES INCIDENCE IN U.S.A. 1973/74. CHILDREN LESS THAN 18 YEARS

	1973	1974
States	Rate per 100 000	Rate per 100 000
With laws	26.5	33.1
Without laws	53.9	55.4

The similarity to Table 4 is obvious. As Lilienfeld and Lilienfeld (1977) remark: "The efforts of the CDC to immunize the population, including their collective reasoning and methods, do not differ from those used 125 to 150 years ago to justify smallpox vaccination programs. One need only substitute the word measles for smallpox in the reports of the last century and they read like modern documents."

REFERENCES

Guy, W.B. (1839). "On the value of the numerical method as applied to science, but especially to physiology and medicine". *J.R. Statist. Soc. Old Series* 1, 25-47.

Holmes, O.W. (1843). "The contagiousness of Puerperal Fever", in *Medical Essays* 1842-1882, Houghton, Mifflin & Co. 1891 (Reproduced in part in King (1971).).

King, L.S. (1971). *A History of Medicine*. Penguin.

Lilienfeld, D.E. & Lilienfeld, A.M. (1977). "Epidemiology: A Retrospective Study." *Amer. Journ. of Epidemiology* 106, 445-449.

Louis, P.C.A. (1836). *Researches on the Effects of Blood-letting in some Inflammatory Diseases, and on the Influence of Tortarized Antimony and Vesication in Pneumonitis*. Translated by C.G. Putman. Boston, Hilliard, Gray and Co.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

$8833 = 88^2 + 33^2$, $221859 = 22^3 + 18^3 + 59^3$,

$34\ 012\ 224 = (3 + 4 + 0 + 1 + 2 + 2 + 2 + 4)^6$.

(Garnet J. Greenbury)

THE TWO FACES OF CODING THEORY

John Stillwell, Monash University

The word "coding", which we could define as any process for converting a message into a sequence of symbols, probably calls to mind examples such as Morse code and the secret codes used by spies. A more modern example, actually more typical of what mathematicians call "coding theory" is the transmission of pictures from spacecraft. To convert a picture into a sequence of symbols, a television camera slices it into rows, then each row into tiny squares, each of which is represented by a symbol which encodes colour and shade. Rows are sent one after another, and a receiver on Earth recovers the picture by reversing the coding process.

These examples raise various objectives one might have in coding a message:

(1) Convenience of transmission.
(2) Protection from random errors (either human, or as a result of "noise" on the transmission line).
(3) Secrecy.
(4) Authenticity (i.e. protection from forgery).

The first objective is fairly easily met, e.g. by Morse code, since Morse is easy to learn and can be sent by almost any means (by telegraph, flashing a torch, smoke signals, etc.). The objectives of secrecy and protection from forgery are certainly *not* met by Morse, since anyone can use it, nor does Morse give much protection from random errors. For example, if one · is erroneously sent as –, the letter H = ···· can be taken as B = –···, F = ··–·, L = ·–·· or V = ···–.

Protection from random errors turns out to be a major mathematical problem, and since World War II a large theory has developed to deal with it. This is what is now called *coding theory*. The problems of secrecy and authenticity are of course much older. Secret codes have existed for thousands of years, and messages have been "signed" and "sealed" in various ways to try and guarantee their authenticity. The traditional term *cryptography* covers the secrecy aspects of coding, but until recently it has remained more of an art than a science. Developments in the 1970's seem likely to change this, and in a later section I shall discuss some fascinating new codes which seem to provide both secrecy and authenticity.

This may lead to cryptography being recognized as the "second face" of coding theory. In coding theory one is trying to protect a message from nature, i.e. from random errors; in cryptography one tries to protect a message from an in-

telligent opponent. In coding theory we can define precisely what degree of protection is achieved, in cryptography we seem on the verge of doing so.

CODING THEORY

If one wants a code which can be easily memorized and sent by hand, then one has to live with a certain percentage of errors. But in an age when large amounts of information are sent electronically and can be processed by computers, it becomes possible to use more complicated coding to detect and *correct* errors automatically.

This seemingly magical process can be explained by an example. Suppose we use two code symbols 0 and 1 to code messages in the English alphabet. The letters can then be coded by the following 26 out of the total of 32 (= 2^5) blocks of 5 code symbols:

A = 00000
B = 00001
C = 00010
D = 00011
⋮
Z = 11001 (= 25, written in binary).

As it stands this code is no more reliable than Morse: for example, if the last 0 in A is wrongly sent we shall receive B = 00001, and perhaps not realize that anything is wrong.

However, suppose we attach a sixth code digit, called a *parity check digit* to each code block. This last digit checks the *parity* (evenness or oddness) of the first five by being 0 if their sum is even, 1 if their sum is odd. The new code is then

A = 000000
B = 000011
C = 000101
D = 000110
⋮
Z = 110011.

Now if a single error is made in a code block, the result will be a block with an odd number of 1's which is therefore *not in the code*. Such a code is called *single-error-detecting*, because a single error in a block can always be detected.

For example, if the fifth digit of A is sent wrongly we will know something is wrong, because 000010 is not in the code. But even assuming there is only one error, we will not be able to correct it, because other code blocks also yield 000010 when one of their digits is sent wrongly.

To be able to correct errors we have to increase the dissimilarity between code blocks. The dissimilarity $d(\alpha,\beta)$ between code blocks α,β is the number of places where α,β differ. For example

$$d(00000,00001) = 1$$
$$d(000000,000011) = 2.$$

The technical term for dissimilarity is *Hamming distance* (named after R.W. Hamming, one of the pioneers of coding theory), and it has the usual geometric properties of distance. In particular, if any distinct α,β in the code have distance $\geqslant 3$, then a single error in α yields an α' which is distance 1 from α but distance $\geqslant 2$ from every other block in the code. Now we can not only detect the error by observing that α' is not in the code, we can also *correct* it by changing α' to the nearest block in the code, namely α. For this reason, a code in which all blocks are at Hamming distance $\geqslant 3$ from each other is called *single-error-correcting*. Similarly, if the distances are $\geqslant 5$ it is *double-error-correcting*, if distances $\geqslant 7$, *triple-error-correcting* and so on.

Of course, when errors are random there may sometimes be more errors in a block than the code is designed to correct. Then choosing the code block nearest to the transmitted block only gives the *most likely* decoding, not necessarily the correct one. However, probability theory shows that the expected number of decoding errors can be made as small as we please by choosing a code with a sufficiently large Hamming distance.

THE MAIN PROBLEM OF CODING THEORY

The real problem of coding theory is not merely to minimize errors, but to do so without reducing the transmission rate unnecessarily. We have seen that errors can be corrected by lengthening the code blocks, but this reduces the number of message symbols that can be sent per second. To maximize the transmission rate we want code blocks which are numerous enough to encode a given message alphabet, but at the same time no longer than is necessary to achieve a given Hamming distance. To put the problem the other way round:

Given block length n and Hamming distance d, find the maximum number, $A(n,d)$, of binary blocks of length n which are at distances $\geqslant d$ from each other.

The following table gives the first few values of $A(n,d)$ for $d = 3$, i.e. the maximum sizes of single-error-correcting codes:

n	3	4	5	6	7	8	9
$A(n,3)$	2	2	4	8	16	20	Not known, but $\geqslant 38$, $\leqslant 40$

The most interesting of these is the code with 16 blocks of length 7, which is one of a family of codes discovered by Hamming. The first four digits z_1,z_2,z_3,z_4 of a block are arbitrary (giving $2^4 = 16$ different blocks), while the last three are determined by the first four, as follows

z_5 = parity check digit for z_1, z_2, z_4

z_6 = parity check digit for z_1, z_3, z_4

z_7 = parity check digit for z_2, z_3, z_4.

Thus in a code block $z_1z_2z_3z_4z_5z_6z_7$ the three sets of digits $\{z_1, z_2, z_4, z_5\}$, $\{z_1, z_3, z_4, z_6\}$ and $\{z_2, z_3, z_4, z_7\}$ must all contain an even number of 1's. It follows that distinct code blocks cannot differ in just 2 places, because for any digits z_i, z_j we can find a set which contains only one of z_i, z_j, and then this set would contain an odd number of 1's for one of the blocks. Thus any two of the 16 blocks in the Hamming code are distance $\geqslant 3$ apart.

To show that no code of length 7 and distance $\geqslant 3$ can have more than 16 blocks we use a geometrical argument. Each code block α has a "neighbourhood $N(\alpha)$ of radius 1", of 8 blocks, namely the 7 blocks α' which differ from α in one place, together with α itself. Since distinct blocks α, β in the code are distance $\geqslant 3$ apart, their neighbourhoods $N(\alpha)$, $N(\beta)$ do not meet. Then the neighbourhoods of the 16 blocks in the code account for $16 \times 8 = 128$ distinct blocks. But there *are* only $128 = 2^7$ binary blocks of length 7, so no more than 16 code blocks at distances $\geqslant 3$ can exist.

A code for which the neighbourhoods (of some fixed radius) around code blocks use up all possible blocks is called *perfect*. If the length of blocks is n, a neighbourhood of radius 1 contains $n + 1$ blocks, and there are 2^n blocks altogether. Thus a perfect single-error-correcting code cannot exist except when $n + 1$ divides 2^n, i.e. when $n + 1$ is a power of 2, or $n = 3, 7, 15, 31, \ldots$. Hamming discovered perfect codes for all these values in 1948. There is *only one* perfect code which corrects more than single errors, a triple-error-correcting code (thus neighbourhoods are of radius 3) with 4096 blocks of length 23, known as the Golay code.

I hope this gives some idea of the mysterious and unexpected phenomena which arise in coding theory. The subject has deep connections with many parts of algebra, geometry and number theory.

CRYPTOGRAPHY

Like coding theory, cryptography deals with the conversion of messages into symbolic form, but the main objective is secrecy. This leads to very different techniques, and a different language is used - "enciphering" instead of "encoding", "deciphering" instead of "decoding". To appreciate the progress made by cryptography in recent years, we shall first look at some of the classical ciphers.

(1) *The Caesar cipher*

According to Suetonius in "The Twelve Caesars", Julius Caesar used a cipher in which each letter of the message was replaced by the letter 3 places later in the alphabet (*X,Y,Z* being replaced by *A,B,C* respectively, of course). In general, a "Caesar cipher" is one in which each letter is replaced by the letter *n* places later in the alphabet, where *n* is some fixed number, called the *shift*.

This kind of cipher is very easy for an opponent to break, since only one cipher letter has to be identified, and all others follow. Identification is possible because letters occur with different frequencies in any natural language. In English the most common letter is *E*, followed by *T, A, O, N, R* and these between them make up more than 50% of the average message, *E* alone making up 13%. In a Caesar ciphered message of only a few dozen symbols one can be fairly sure that the most common letter represents *E*, and deciphering is then immediate.

(2) *Vigenère*

Invented in 1586 by a Frenchman, Blaise de Vigenère, this cipher was considered unbreakable in its day. As in the Caesar cipher, a shift is applied to the alphabet, but the length of shift varies, usually in a periodic way. For example, our opponent might decide to use shifts of lengths 1, 7, 4, 13, 5 over and over again. He then writes the sequence

1, 7, 4, 13, 5, 1, 7, 4, 13, 5, 1, 7, 4, 13, 5, ...

(call this the *key* sequence) for as long as necessary and "adds" it to the message, say

Message	S	E	N	D	M	O	R	E	M	E	N	A	N	D	M	O	R	E	A	R	M	S
Key sequence	1	7	4	13	5	1	7	4	13	5	1	7	4	13	5	1	7	4	13	5	1	7
Ciphered message	T	L	R	Q	R	P	Y	I	Z	J	O	H	R	Q	R	P	Y	I	N	W	N	Z

The changing shifts even out the overall letter frequencies, defeating the kind of analysis used to break Caesar ciphers, but the characteristic frequences are retained in subsequences of the ciphered message corresponding to repetitions in the key sequence (every 5 places in the above example). If we can find the length of the key's period, letters can be identified by frequency analysis as above.

The period can indeed be discovered, by looking for repeated blocks in the ciphered message. Some of these will be accidental, but a large proportion will result from matches between repeated words or subwords of the message and repeated blocks in the key sequence. When this happens, the distance between repetitions will be a multiple of the period. In our example, the block *RQRPYI* is undoubtedly a true repeat; the distance between its two occurrences is 10, indicating that the period length is 10 or 5. Examining all the repeats in a longer ciphered message, we will find a majority at distances which are multiples of 5, at which time we will know that the period is 5.

(3) *One time pad.*

The ultimate generalization of the Vigenère was proposed by the American engineer G.S. Vervam in 1926, namely, let the key sequence be arbitrarily long and *random*, and use successive blocks of it for successive messages. This is a cumbersome method, because both sender and receiver need to keep a copy of the long key sequence, but it is clearly unbreakable - the randomness of the key means that any two message sequences of the same length are equally likely to have produced the ciphered message.

A one time pad is used for the hot line between Washington and Moscow.

The increase in security from Caesar cipher to one time pad depends on increasing the length of the key. For a Caesar cipher the key is a single number between 1 and 26 (the length of shift), for a periodic Vigenère a finite sequence of numbers, for the one time pad a potentially infinite sequence. The longer the key, the harder the cipher is to break, but for all the classical ciphers it is possible for an opponent to reconstruct the key by an amount of work which does not grow too exhorbitantly relative to key size.

This situation was seen in a new light with the rise of computational complexity theory in the 1970's (sèe my article "Why mathematics is difficult" in *Function*, Volume 4, Part 3). Mathematicians became aware of many "one-sided" problems, whose short and easily checked answers were nevertheless very difficult to find. Diffie and Hellman, of Stanford University, suggested in 1977 that such problems might provide ciphers whose keys cannot be feasibly reconstructed by an opponent, even though they are relatively short and convenient for an authorized decipherer to use.

Using a "one-sided" (or "trapdoor", as Diffie and Hellman call it) problem as basis for a cipher means that the key for enciphering can be made public without giving away the key for deciphering, since an opponent who does not know the answer to the problem cannot find it except by an infeasibly long computation.

The most famous such cipher, invented by Rivest, Shamir and Adleman at the Massachusetts Institute of Technology, is based on the factorization problem. One takes two large prime numbers q_1, q_2 of about 100 digits each, and uses their product $P = q_1 q_2$ for enciphering, the factors q_1, q_2 for deciphering (for details, see Rod Worley's article "Primes" in *Function*, volume 3, part 5 or Martin Gardner's column in *Scientific American*, August 1977). Since no feasible method is known for factorizing large numbers, it is possible to make P public without giving away q_1 and q_2. It has been proved that any method of breaking the Rivest-Shamir-Adleman cipher is equivalent to finding q_1 and q_2, so the factorization problem has suddenly become very important applied mathematics. If it can be proved that factorization is inherently difficult, we will finally have ciphers to put professional codebreakers out of business.

PUBLIC KEY CRYPTOSYSTEMS

Diffie and Hellman describe the desirable features of a cipher in terms of an enciphering procedure E and a deciphering procedure D, as follows:

(a) Deciphering an enciphered message M yields M, i.e.

$$D(E(M)) = M.$$

(b) E and D are easy to compute.

(c) E can be made public without revealing D; more precisely, D cannot be constructed from E without solving a computationally infeasible problem.

(d) It makes sense to decipher any message M, and enciphering the result yields M, i.e.

$$E(D(M)) = M.$$

Considerable number theory is needed to establish (a), (b), (d) for the Rivest-Shamir-Adleman cipher and, as we have said, it is not yet established that (c) is true (i.e. that factorization is infeasible) for that particular cipher. Nevertheless, in the reasonable expectation that such ciphers exist, Diffie and Hellman call them *public key cryptosystems*, and point out some interesting applications.

To begin with, any person B (Bob, say) who wants to receive messages can place his enciphering method, E_B, in a public directory (like a telephone directory), enabling anyone else to communicate with him in guaranteed privacy, since only B has the deciphering method, D_B.

B can also "sign" messages he sends to another person A (Alice, say), so that A is assured of their authenticity. To sign a message M, B first computes the "digital signature"

$$S = D_B(M) ;$$

then, if he is communicating with A, looks up E_A in the directory and sends $E_A(S)$. He also sends the uncoded message that he, B, is the author of the message. A will be able to check the truth of that, as we shall see. Since A has the deciphering procedure D_A, she can first compute

$$D_A(E_A(S)) = S,$$

obtaining the signature S, then use E_B from the directory to obtain the message M:

$$E_B(S) = E_B(D_B(M)) = M.$$

Since only B can have created an S which deciphers to M by E_B, A knows that M can only have come from B.

(Here we are assuming that only a tiny fraction of symbol sequences actually are meaningful messages M, as is the case for sequences of letters in the English alphabet. Then any forgery S' is likely to be detected, because of the miniscule probability that $E_B(S')$ will be a meaningful message M'. This protection against forgery is analogous to the way error-correcting-codes give protection against random errors, namely, by having only a small fraction of possible binary blocks actually in the code.)

Here are two uses for digital signatures.

(1) *Electronic banking.*

B can send and sign a cheque M to A, electronically, so that A not only knows that the cheque is genuine, she can also convince the bank of it. In fact, A can show that bank the calculation $E_B(S) = M$ which proves the authenticity of the cheque, while keeping to herself the procedure D_A by which she obtained S from the $E_A(S)$ sent by B!

(2) *Monitoring nuclear tests.*

A test ban treaty between the U.S. and Soviet Union proposes that each nation place seismic instruments in each other's territory, to record any disturbances and hence detect underground tests. It is possible to protect the instruments (in the sense that they can be made to self-destruct if anyone tampers with them) but not the channel which sends their information (the host nation could cut the wires and send false information). Furthermore, if information is sent in ciphered form, the host nation may suspect that unauthorized information is also being sent, in addition to the agreed-on seismic data.

A digital signature system is the ideal solution to this problem. Nation B's seismic station contains a computer which coverts the message M to

$$S = D_B(M).$$

Nation A cannot substitute anything S' for S, because of the overwhelming probability that $E_B(S') = M'$ will not be meaningful, and hence nation B will detect the forgery. However, nation B *can* supply A with the procedure E_B, which A can then use to recover

$$M = E_B(S),$$

and thus be reassured that only an authorized message M is being sent.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

Decipher:

J LRWTZLH WTIU'W NWUPGYZ.

(Vigenère)

WHERE DID CONIC SECTIONS COME FROM?

H.K. Kaiser
Technische Universität, Vienna

Most of the elementary concepts of mathematics have their origins in the world around us. Several attempts have been made to trace back the roots of the concept of number and the basic objects occurring in geometry. In this context one may ask why people started to investigate conic sections. It may be argued that conic sections appear in the world around us since they can be used in describing the movement of the planets. But this was discovered by Kepler only 2000 years *after* the first discussion of this concept. Or one might say that some of the architects of antiquity must have been familiar with ellipses as oblique sections of cylindric columns, but -as we shall see - it was the parabola and the hyperbola which were first treated from a mathematical point of view. Are conic sections perhaps just an invention of some ingenious mathematician as some form of "general abstract nonsense" who was acting like a "spider who is spinning its web from its own substance"? This metaphor is due to Roger Bacon (ca. 1219-1292). Or do we have to believe one of the Greek philosophers who claimed that all of geometry was created by some Egyptian god, Thoth?

In order to find out why the ancient Greeks considered conic sections at all we first take a closer look at Greek geometry. Quite a lot of higher Greek geometry has its origins in attempts to solve the three "classical" problems of Greek mathematics:

1. *The duplication of a cube (to construct the edge of a cube having twice the volume of a given cube).*
2. *The trisection of an angle (to find a construction for dividing any given angle into three equal parts).*
3. *The quadrature of the circle (for any circle to construct a square of equal area).*

The real scientific stimulus of these problems was the restriction on the constructions which were permitted in solving the problems. One was only allowed to use the (unmarked) ruler and the compass - the so-called Euclidean tools - for the various constructions. Euclid states some postulates at the beginning of his "Elements" which describe the constructions one is allowed to perform when doing "precise" geometrical investigations:

P1. *It is possible to draw a straight line from any point to any other point.*

P2. *It is possible to produce a finite straight line indefinitely in that straight line.*

P 3. It is possible to describe a circle with any point as centre and with a radius equal to any finite straight line drawn from the centre.

Perhaps it is worthwhile mentioning that Euclid never uses the words ruler or compass in his work. It would not have fitted in with his attitude towards mathematics because with these tools one would only be able to give an approximation of the actual geometric truth.

So this leaves us with another question. Why did the Greek mathematicians want to find solutions of the three problems with Euclidean tools alone? (For all three problems such a solution is impossible as we now know by the brilliant work of E. Galois and C. Lindemann, two mathematicians of the nineteenth century). To answer this question we have to go right back to the beginning of Greek mathematics.

One of the great achievements of ancient Greece was the creation of mathematics or, to be more precise, of geometry, as a science. They erected a system which was based on simple statements which were generally accepted to be true. In this system other, more complicated, statements were proved to be true by *reasoning*. This development of the science of geometry started around 600-500 B.C. and is connected with the first Greek mathematicians we know by name: Thales and Pythagoras. It took more than 200 years to complete this system, which was achieved in the work of Euclid around 300 B.C. The main source about the early stages of Greek mathematics (up to Euclid) is the "History of Geometry" in four books by Eudemus (ca. 335 B.C.). Unfortunately his original work is lost and we only know of it by the "Eudemian summary" of Proclus (410-485 A.D.), which is found at the beginning of his "Commentary on Euclid, Book I".

Pythagoras founded a school of mathematics in Magna Graecia (southern Italy). The Pythagoreans tried to express everything by means of numbers or ratios of numbers. Here "number" just means "positive integer". Their philosophy rested on the assumption that whole numbers are the cause of the various qualities of man and matter. The program of studies was based on arithmetic, geometry, music and astronomy: the four "mathematical" liberal arts. But their philosophy that numbers are the essence of the world was soon shattered by the discovery of irrationals. The Pythagoreans were not able to express such a familiar thing as the length of the diagonal of a square of unit length in terms of natural numbers and they even found out that this was impossible to achieve. In essence they probably used the same reasoning as we do today to show that $\sqrt{2}$ is not a rational number:

Suppose that $\sqrt{2} = \frac{m}{n}$, m and n relatively prime, positive integers (hence at least one is odd), then we have $m^2 = 2n^2$. Hence m is even, say of the form $2r$. But then $2r^2 = n^2$, so n is even. Since "something even cannot be equal to something odd", the assumption that $\sqrt{2}$ could be represented as a ratio of numbers was wrong.

So the Pythagoreans said that "$\sqrt{2}$ has no ratio", or is irrational. From this they concluded that precise mathematics could not be based on numbers alone and tried to give mathematics a new precise foundation. The obvious starting point for them was geometry since there one could easily represent $\sqrt{2}$ as the length of a line segment, and this was even possible for any

arbitrary (finite) magnitude. One could easily perform addition and subtraction of magnitudes in the geometrical setting. The operation of multiplication was just represented by forming rectangles and division (e.g. $x = a \div c$) required the construction of a rectangle cx, with c given, which was equal to a given rectangle with sides a and 1. Thus the Pythagoreans achieved a general framework for their mathematical investigations. But still they used their theory of proportions, based on numbers, which of course was not able to cope with irrationalities properly. They seem to have justified the application by dividing the magnitudes into infinitely small parts. But this aroused the criticism of philosophers like Zeno of Elea (around 450 B.C.), who showed in a very striking way the logical difficulties the Pythagoreans had run into. Should one assume that a magnitude is infinitely divisible or that it is made up of a very large number of small indivisible atomic parts? Let us look at two paradoxes which assert that motion is not possible if we adopt either one of the two assumptions:

The dichotomy: *If a straight line segment is infinitely divisible then motion is impossible,* for in order to traverse the line segment it is necessary first to reach the midpoint, and to do this one must first reach the one-quarter point, and to do this one has to first reach the one-eighth point, and so on to infinity. It follows that motion can never begin.

The arrow: *If time is made up of indivisible atomic instants, then a moving arrow is always at rest,* for at any instant the arrow is in a fixed position. Since this is true of every instant, it follows that the arrow never moves.

As a consequence, Greek mathematicians excluded infinitesimals from their discussions. So in the time of Plato (427-347 B.C.) mathematicians needed new concepts to give their science a logically correct foundation. This was mainly done by Theaetetus (ca.375 B.C.) and Eudoxus of Knidos (ca.370 B.C.). The latter gave the following definition of proportion or equality of ratios:

> *Magnitudes are said to be in the same ratio, the first to the second and the third to the fourth, when, if any equimultiples whatever be taken of the first and third, and any equimultiples whatever of the second and fourth, the former equimultiples alike exceed, are alike equal to, or are alike less than the latter equimultiples taken in corresponding order.*

In other words: If A, B, C, D are any magnitudes, A and B of the same kind (both line segments, or angles, or areas etc.) and C and D of the same kind, then the ratio of A to B is equal to that of C to D when for arbitrary positive integers m and n, $m\,A \gtreqless n\,B$ according as $m\,C \gtreqless n\,D$.

So here was a tool adequate for tackling irrationalities. The problem of infinity was dealt with by making use of the famous exhaustion principle, in which the infinite divisibility of magnitudes is assumed:

> *If from any magnitude there be subtracted a part not less than its half, from the remainder another part not less than its half, and so on, there will at length remain a magnitude less than any preassigned magnitude of the same kind.*

The whole system of Greek geometry, based on these new foundations was written up by Euclid in his "Elements". His treatment remained the model of rigorous mathematical investigation for a long time. The principle was to state all assumptions of the investigation in a precise way at the beginning. Euclid starts his "Elements" with definitions, which introduce the names of the concepts without stating what these concepts actually were. This was done by postulates which are a list of properties characterizing the concepts in question. Then he states his assumptions (or axioms) which are generally agreed on. Axioms are for example:

> *A1. Things which are equal to the same thing are also equal;* or
>
> *A2. If equals be added to equals, the wholes are equal.*

Euclid's axioms, postulates and definitions for plane geometry restricted the constructions allowed in a rigorous mathematical treatment of a problem to the constructions which one could perform according to these assumptions, in other words to constructions with unmarked ruler and compass. This explains the continued attempts to solve the three classical problems merely by using the Euclidean tools. No solution by other means would have been accepted, for a quantity was only taken to have a geometric existence if its construction from the basic postulates could be precisely achieved.

Let us now return to the question of the origin of conic sections. For this we turn our attention to the problem of the duplication of the cube. Our main source on the history of this problem is Eutocius (ca. 560 A.D.), one of the commentators on the works of Archimedes. He reports on a letter from Eratosthenes to King Ptolemy, which starts as follows:

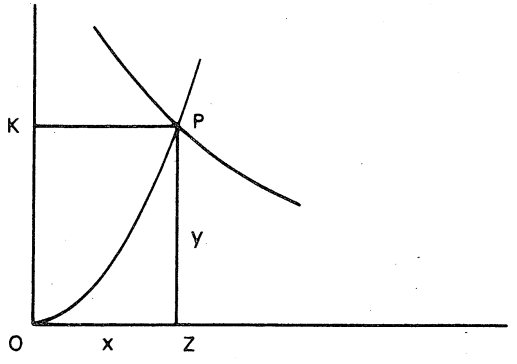
"It is said that one of the ancient tragic poets brought Minos on the scene, who had a tomb built for Glaucos. When he heard that the tomb was a hundred feet long in every direction he said: "You have made the royal residence too small, it should be twice as big. Quickly double each side of the tomb without spoiling the beautiful shape". He seems to have made a mistake. For when the sides are doubled, the area is enlarged fourfold and the volume eightfold. The geometers then started to investigate how to double a given body without changing its shape, and this problem was called the duplication of the cube, since they started with a cube and tried to double it. After they had looked for the solution in vain for a long time, Hippocrates of Chios observed that, if only one could find two mean proportionals between two line segments, of which the larger one is double the smaller, then the cube would be duplicated. This transformed the difficulty into another one, no less great. It is further reported that after some time, certain Delians, whom an oracle had given the task of doubling an altar, met the same difficulty. They sent emissaries to the geometers in Plato's Academy to ask

them for a solution. These took hold with great diligence of the problem of constructing two mean proportionals between two given lines. It is said that Archytas solved it with half cylinders, Eudoxus with so-called curved lines."

So here we are told of Hippocrates' transformation of the problem of duplicating the cube, which asks for the construction of two mean proportionals x and y between given line segments of length s and $2s$. So one has to solve:

$$s : x = x : y = y : 2s, \text{ because then } y^3 = 2x^3.$$

Menaechmus (around 350 B.C.) gave another solution for finding the two mean proportionals. Given a and b we want to find x, y such that $a : x = x : y = y : b$. We lay off $OZ = x$ and $ZP = y$. Our proportion yields $x^2 = ay$, hence P lies on a "parabola" with vertex O.

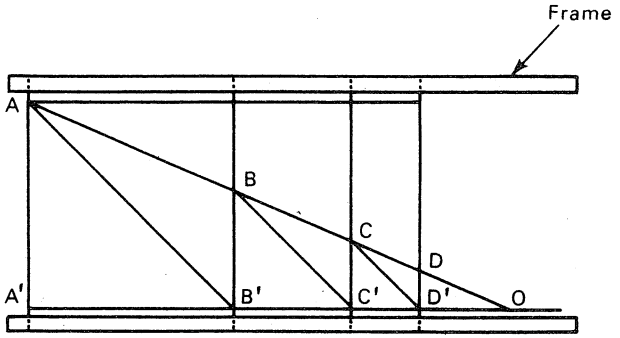


Similarly we get $xy = ab$, hence P is on a "hyperbola" with asymptotes OZ and OK. Therefore P can be found by intersecting the two "curves" and conversely, the proportion follows from the equations of the two "curves".

But of course, the Greek mathematicians did not accept this solution as an exact one. Plato is said to have complained about the various attempts to reduce the duplication to mechanical constructions, because "these were non-theoretical methods which destroyed the good in geometry". Plato was very interested in mathematics and some historians assert that he wanted to lead the mathematicians of his Academy to a more systematic cultivation of solid geometry. What did Plato mean by "solid geometry"? In one of his works, the "Epinomis", we read: plane geometry is defined as the science which teaches us how to make similar two (plane) numbers which are not themselves similar. Here two numbers ab and cd are called similar if $a : b = c : d$, in other words, two numbers considered as areas of rectangles are similar if the sides of the rectangles are proportional. In the eighth book of the "Elements" we find a characterization of similarity: two numbers are similar only if a mean proportional exists between them.

So plane geometry teaches us how to transform any rectangle into a square by means of the operations of geometric algebra. Now, Plato thinks of solid geometry as a generalization of geometric algebra to space. Two spatial numbers (consisting of three factors) *abc* and *def* are called similar if $a : d = b : e = c : f$ and solid geometry is just defined as the science which tells us how to make similar two such numbers which are not themselves similar. So solid geometry deals with the solution of equations like $x^3 = V$, $x^2 (x + a) = V$ and the like. Now we understand why the duplication of the cube (more precisely the enlargement of the cube in a given ratio) was considered to be *the* problem of solid geometry.

Numerous solutions of this problem became known in antiquity. One of them is due to Eratosthenes which he engraved on a stone, which had on top a model of the mechanical instrument he devised for his solution. This model consisted of three rectangular plates which could be moved back and forth between a fixed and a rotating ruler.



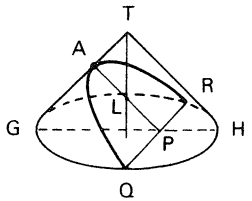
Here is the text of the engraving:

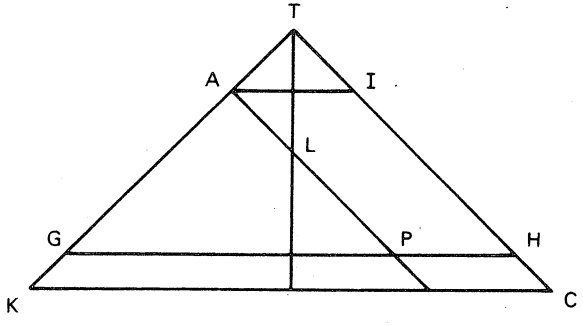
> *To determine two mean proportionals in continued proportion to two given lines. Let the lines AA' and DD' be given. Then move the plates of the instrument towards each other until the points A,B,C,D all lie on one line. Since AA' and BB' are parallel, OA and OB have the same ratio as OA' and OB'. And since AB' and BC' are parallel this ratio also equals that of OB' and OC'. Hence OA' is to OB' as OB' is to OC'. But AA' and BB' also have the same ratio, as well as BB' and CC'. In the same way we prove that BB' is to CC' as CC' is to DD'. Therefore AA', BB', CC' and DD' form a proportion. Thus two mean proportionals between two given lines have been found. If now the given lines are not equal to AA' and DD', we shall obtain the mean proportionals by marking AA' and DD' proportional to them; we reduce them to these and thus the task*

will have been carried out. In case more mean proportionals have to be found, every time we take one more plate in the instrument than the number of mean proportionals to be constructed. The proof remains the same.

Other mechanical devices for the solution of the duplication problem have been found. The interested reader is referred to e.g. H. Eves: Introduction to the history of mathematics, chapter IV. Let us return to the solution by Menaechmus. In order to make his solution acceptable to the mathematical world of his time he had to find a way to present his "curves" in a precise geometric way. So he had to give a description of the construction of his curves without leaving the generally accepted principles of the elementary geometry of solids. Menaechmus' main observation was that each such curve occurs as the intersection of a right circular cone with a plane perpendicular to its generating line. If one takes a rectangular right circular cone one obtains a parabola, in the case of an acute angled one an ellipse, and for obtuse angled cones a hyperbola.

How did Menaechmus find the "symptoms" (equations) of his conic sections? We can only guess. In the case of the parabola perhaps his thoughts ran along the following lines:





Let TKC be a plane through the axis and at right angles to the base of a right circular right-angled cone with vertex T and generating line TK. Let AP be the line of intersection with a plane which is perpendicular to TK. We project onto P (which is a point in our plane of drawing) two points Q,R of the curve which is determined by the intersection of this plane and the given cone. Let y be the distance $QP = RP$ and let AP be x. We draw AI and GPH parallel to KC. Then we have:

$$y^2 = GP.HP \text{ (by theorems of Thales and Pythagoras)}$$

$$= \sqrt{2}.AP.HP \text{ (since } AG = AP \text{ and } \sphericalangle GAP \text{ is a right angle)}$$

$= \sqrt{2}.AP.AI$ ($APHI$ is a parallelogram)

$= \sqrt{2}.AP.\sqrt{2}.AL$ ($ALIT$ is a square)

$= 2.AL.x$,

where L denotes the intersection of the plane and the axis of the cone. Since $2AL = 2AT$, this is a constant and we set: $2AL = p$. This yields $y^2 = px$, the familiar equation of the parabola. Conversely, every curve which is determined by $y^2 = px$ can be represented as a section of a right-angled right circular cone by marking off $TA = \frac{1}{2}p$ on the generating line TK of the cone.

Before the time of Apollonius, who wrote the most mature treatise on conic sections of ancient times, the three conic sections were usually called "triads of Menaechmus" or just sections of right-angled, acute-angled or obtuse-angled cones. This terminology is an indication that Menaechmus was not so much interested in the study of conic sections for its own sake as to show that these curves really existed in a mathematical sense. Otherwise he would probably have represented his curves as intersections of one cone with planes at an arbitrary angle to the generating line. This was done later by Apollonius who also introduced the names for the conic sections with which we are familiar.

So, this is the story how conic sections became an object of mathematical investigation - at least as it is told by the ancient Greeks. The Greek mathematicians gave conic sections considerable attention. If you want to find out more about the way Archimedes and Apollonius discussed them I recommend you read B.L. van der Waerden's book "Science Awakening" (P.Noordhoff Ltd. Groningen 1961). Or, if you like problem solving, try to design your own instrument for finding mean proportionals between given line segments and thus invent your personal method for duplicating a cube!

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

... Dad could multiply large numbers in his head, without using pencil and paper ... . [For example, to] multiply forty-six times forty-six, you figure out how much greater forty-six is than twenty-five. The answer is twenty-one. Then you figure out how much less forty-six is than fifty. The answer is four. You can square the four and get sixteen. You put the twenty-one and the sixteen together, and the answer is twenty-one sixteen, or 2116.

F.B. Gilbreth and E.G. Carey,
Cheaper by the Dozen, 1949.

∞ ∞ ∞

$x < y$ or $y < x$?

"Just in case Essendon's Tim Watson wins the Brownlow Medal on Monday night here's a fact which will save everyone racing for the record books.

Watson was 19 on 13 July, but he would not be the youngest Medal winner. That honor would still be with Essendon's great Dick Reynolds, who was 19 on June 20, 1934, the year he won the first of three Brownlows."

The Age, 18.9.1980.

LETTER TO THE EDITORS

I wish to submit a calculator program for publication in your magazine. This program is for the Texas Instruments TI58C or TI59 programmable calculators and is a game called "Splat". Basically, the game simulates a parachutist descending over the surface of a planet; the object of the game being to open the parachute as close as possible to the ground and to avoid hitting the ground before the parachute is opened. The parachutist descends over different planets, and the calculator randomly selects the acceleration due to gravity, the height and the velocity at which the parachutist is thrown downwards.

Programmable calculators are becoming very popular with high school students and I believe that this particular type of programmable calculator is the most popular among students owning programmable calculators. So I believe that this program would be worth publishing. I would also like other students to send in their programs or programming ideas. I would like your magazine to be more computer orientated, since computers play a great part in mathematics today. I hope that you will publish my program in one of your forthcoming issues.

Ravi Sidhu,
131 Marabou Drive,
Townsville, Queensland, 4814.

SPLAT

(A game for the Texas Instruments TI58C or 59 programmable calculators.)

Instructions:

You are being dropped from a space-craft over the surface of a certain planet. By entering a number between 0 and 199017 and pressing *A* on the calculator, a value for the acceleration due to gravity for that planet will be displayed. By pressing *B* your height above the planet will be displayed and by pressing *C* the velocity at which you are thrown downwards will be displayed. All these numbers are generated randomly by the calculator. You will be free-falling for a certain length of time and then your parachute will open. You are to enter the time for which you wish to free-fall by pressing *D* after entering the number. Your parachute will open at the end of this time. The object of the game is to open your parachute as close as possible to the ground. You start your descent by pressing *E*. Ten samples of your height will be displayed during the descent. For each, the time will be shown first, followed by your height above the ground. When your parachute has opened, the program will stop and your height above the planet will be displayed. If you hit the ground before your parachute opens, the calcu-

lator will flash "99999999 99" on the display, indicating that you are splattered over the surface of the planet.

(The calculator is not allowed to be used to calculate your guess for the time.)

acceleration is in m/s^2
height is in metres
starting velocity is in m/s.

(The program is 120 steps long, and uses memory registers 1 to 11 and 19 to 29.)

```
000 76  Lbl
001 11  A
002 47  CMs
003 36  Pgm
004 15  15
005 15  E
006 36  Pgm
007 15  15
008 71  SBR
009 88  D.MS
010 65  ×
011 02  2
012 00  0
013 95  =
014 59  Int
015 42  STO
016 20  20
017 91  R/S
018 76  Lbl
019 12  B
020 36  Pgm
021 15  15
022 71  SBR
023 88  D.MS
024 65  ×
025 03  3
026 00  0
027 00  0
028 00  0
029 95  =
030 59  Int
031 42  STO
032 21  21
033 42  STO
034 19  19
035 91  R/S
036 76  Lbl
037 13  C
038 36  Pgm
039 15  15
040 71  SBR
041 88  D.MS
042 65  ×
043 01  1
044 00  0
045 00  0
046 95  =
047 59  Int
048 42  STO
049 22  22
050 91  R/S
051 76  Lbl
052 14  D
053 42  STO
054 23  23
055 55  ÷
056 01  1
057 00  0
058 95  =
059 42  STO
060 26  26
061 91  R/S
062 76  Lbl
063 15  E
064 43  RCL
065 26  26
066 44  SUM
067 25  25
068 43  RCL
069 23  23
070 32  x⇌t
071 43  RCL
072 25  25
073 67  x=t
074 17  B'
075 77  x≥t
076 19  D'
077 76  Lbl
078 17  B'
079 66  Pause
080 43  RCL
081 19  19
082 75  -
083 53  (
084 43  RCL
085 25  25
086 65  ×
087 43  RCL
088 22  22
089 85  +
090 93  .
091 05  5
092 65  ×
093 43  RCL
094 20  20
095 65  ×
096 43  RCL
097 25  25
098 33  x²
099 54  )
100 95  =
101 42  STO
102 21  21
103 29  CP
104 22  INV
105 77  x≥t
106 18  C'
107 66  Pause
108 66  Pause
109 15  E
110 76  Lbl
111 18  C'
112 25  CLR
113 35  1/x
114 91  R/S
115 76  Lbl
116 19  D'
117 43  RCL
118 21  21
119 91  R/S
```

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

MATHEMATICAL MODELS IN POPULATION GENETICS

Simon Tavaré, University of Utah

Population genetics is one of many biological fields in which mathematical models have played a significant role. Although such models do not claim to be precise descriptions of reality, they are nonetheless useful in assessing the roles of separate parts of the real process under study. In this article, we describe some of the simpler genetic models. We will indicate briefly the methods that may be used to analyse them, and the results that follow.

The study of theoretical population genetics attempts to quantify how the genetic constitution of a population changes with time. We will suppose that each individual in the population under study is one of three possible genetic types, denoted by *AA*, *Aa* and *aa*. We call the classifications *AA*, *Aa*, *aa* *genotypes*. Any individual inherits one *gene* (either *A* or *a*) from each of his parents. For example, if one parent is *AA* and the other *Aa*, then the offspring are *AA* or *Aa*, each with chance $\frac{1}{2}$. If the population is a type of sweet pea, and *A* is the gene for red flowers, *a* the gene for white flowers, then *AA* flowers are red, *aa* white and *Aa* are pink. Further details of elementary genetics are provided in reference [1] below.

We say that our population exhibits (genetic) *variation* if both the genes *A* and *a* are present in that population. This genetic diversity should allow the population to adapt more readily to its surroundings.

THE HARDY-WEINBERG LAW

The simplest result about the genetic makeup of the population is provided by the celebrated Hardy-Weinberg Law [3,4]. For simplicity we will assume that generations are discrete: at each time point all individuals die, and are replaced by new individuals at the next time point. Now suppose that the three genotypes *AA*, *Aa*, *aa* are represented in proportions D, $2H$, R respectively ($D + 2H + R = 1$). The fraction of *A* genes is denoted by p, and is given by $p = D + \frac{1}{2}.(2H) = D + H$. To compute the proportions D', $2H'$, R', p' in the next generation, we use the mating table opposite.

Mating table

mating type	proportion	fraction of offspring of type AA	Aa	aa
$AA \times AA$	D^2	1	0	0
$AA \times Aa$	$4DH$	$\frac{1}{2}$	$\frac{1}{2}$	0
$AA \times aa$	$4DR$	0	1	0
$Aa \times Aa$	$4H^2$	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$
$Aa \times aa$	$4HR$	0	$\frac{1}{2}$	$\frac{1}{2}$
$aa \times aa$	R^2	0	0	1

The proportion D' of AA genotypes is given by

$$D' = D^2.1 + 4DH.\tfrac{1}{2} + 4H^2.\tfrac{1}{4} = (D + H)^2 = p^2$$

while $2H' = 2p(1 - p)$, $R' = (1 - p)^2$. Also note that $p' = D' + H' = p$. Repeating the previous argument in the next generation shows that $D'' = p^2$, $2H'' = 2p(1 - p)$, $R'' = (1 - p)^2$, and the same proportions are maintained in all subsequent generations.

This result is extremely important. Assuming there are no external pressures (such as are caused by one genotype being more successful in producing offspring than others) acting on the population, genetic variation is maintained. Notice that the fraction, p, of A genes is constant in *all* generations.

We now turn to the 'external pressures' mentioned above. We refer to the different survival or mating success of the three genotypes as *selection*. How does selection affect genetic variation?

THE ROLE OF SELECTION

We will introduce three positive numbers w_{AA}, w_{Aa}, w_{aa} which are called the relative *fitnesses* of the genotypes. They are used to model the effect of different viability and fertility among the genotypes. If, for example, AA genotypes are more successful (at reproducing or surviving) than aa genotypes, then w_{AA} is larger than w_{aa}. Let p_n be the proportion of A genes in generation n, and let $q_n = 1 - p_n$, $n = 0,1,2,\ldots$. A mating table similar to the previous one can be used to show that p_{n+1} is related to p_n by the formula

$$p_{n+1} = \frac{p_n(w_{AA}p_n + w_{Aa}q_n)}{p_n^2 w_{AA} + 2p_n q_n w_{Aa} + q_n^2 w_{aa}}, \quad n = 0,1,2,\ldots . \qquad (*)$$

Notice that if $w_{AA} = w_{Aa} = w_{aa}$, then $p_{n+1} = p_n = \cdots = p_0$, which is the Hardy-Weinberg case we have already encountered.

Equations like (*) are called recurrence relations, and they play an important part in mathematical modelling. From our point of view the interesting question to ask is: What happens to p_n after a large number of generations? In principle, this is not a simple question to answer, but we will illustrate what happens in some specific cases.

Case (a) $w_{AA} = 0$, $w_{Aa} = w_{aa} = 1$.

This is a model in which AA-individuals cannot reproduce. Examination of (*) in this special case shows that

$$p_n = p_{n-1}/(1 + p_{n-1}), \quad n = 1,2,\ldots .$$

Whence

$$p_n = \frac{p_{n-2}}{1 + 2p_{n-2}} = \ldots = \frac{p_0}{1 + np_0}, \quad n = 0,1,2,\ldots .$$

This shows that p_n approaches 0 as n increases. Thus variation tends to be lost, in that the population will eventually comprise only aa-individuals. To determine how long it takes to reduce the fraction of A genes from p_0 to p, we have to solve for n the equation $p = p_0/(1 + np_0)$, giving $n = p^{-1} - p_0^{-1}$. For example, if $p_0 = \cdot 5$, it takes 8 generations to reduce the fraction to $\cdot 1$ and 998 generations to reduce it to $\cdot 001$. Although the A-gene must disappear, it may take a long time.

Case (b) $w_{AA} = w_{aa} = 1$, $w_{Aa} = 2$.

Since individuals who have both genes A and a are fittest, it is likely that both genes will survive. We might expect the proportion p_n to stabilise to some value p^* as n increases. For example, if $p_0 = \cdot 9$, then $p_5 = \cdot 595$, $p_{10} = \cdot 513$, $p_{15} = \cdot 502$, $p_{20} = \cdot 5002$, suggesting that $p^* = \cdot 5$. In fact, starting from any p_0 between 0 and 1, p_n approaches $\cdot 5$ as n increases.

The importance of this example is that it shows that *both* genes are maintained in the population, although we no longer have the constant proportions given in the Hardy-Weinberg Law. Eventually the population will comprise AA, Aa, aa in proportions $\frac{1}{4}$, $\frac{1}{2}$, $\frac{1}{4}$ respectively.

MUTATION

Another genetic factor we have to allow for is mutation. Suppose that it is possible for A genes to change into a genes. In any generation, an A gene has a chance v ($0 < v \leqslant 1$) of becoming an a gene. We will ignore the possibility of a changing into A. The recurrence relation for p_n is given by

$$p_n = p_{n-1}(1 - v), \quad n = 1,2,\ldots . \qquad (**)$$

This is derived by noting that the proportion p_n of A genes at time n is the proportion p_{n-1} at time $n - 1$ times the chance $1 - v$ that the A's do not mutate. From (**) it is clear that

$p_n = (1 - v)^n p_0$, and hence that p_n approaches 0 as n increases. This confirms the intuitive result that the A gene must eventually be eliminated.

To assess how strong the mutation force is, we can compute the time n required to reduce the A gene fraction from p_0 to p. We solve for n the equation $p = (1 - v)^n p_0$, leading to $n = \log_e(p/p_0)/\log_e(1 - v)$. For illustration, we take $p_0 = \cdot 5$ and $v = 10^{-6}$ (a typical value of the mutation rate in man). The time to reduce the fraction to $\cdot 1$ is $1 \cdot 61 \times 10^6$ generations, and to $\cdot 001$ it is $6 \cdot 21 \times 10^6$ generations. Comparing these results with those obtained in case (a), we conclude that selection can be a much stronger force in eliminating (genetic) variation than mutation.

SMALL POPULATIONS

The previous models have assumed that the population we are studying is very large. We might then enquire what effects small population size have on the previous results. The mathematical models are now much more complicated to analyse, see [2], but the following results indicate what can happen.

We consider a population of N individuals, each classified as one of the three genotypes AA, Aa, aa. To keep things manageable, we keep track only of the number of A genes, and not how these are arranged in individuals. Our population can then contain any of $X = 0,1,\ldots,2N$ A genes, the remaining $2N - X$ being a genes.

Before describing our model, we digress briefly to review some properties of the *binomial* distribution. Suppose we perform a series of n coin-flips, in each of which we have probability p of throwing a head, and $q = (1 - p)$ of throwing a tail. Then the chance of tossing $X = k$ heads is given by

$$\text{Prob}(X = k) = \binom{n}{k} p^k q^{n-k}, \quad k = 0,1,\ldots,n, \qquad (***)$$

where $\binom{n}{k}$ is the binomial coefficient, $\binom{n}{k} = \frac{n!}{k!(n - k)!}$. The random variable X is said to have a binomial distribution with parameters n and p. Let's return to our genetic problem.

The model for the number of A genes in the next generation is derived as follows. If in generation n the number of A genes is i, then the proportion is $p_n = i/2N$. To produce the genes in generation $(n + 1)$, we take a binomial sample of size $2N$ from a very large pool of genes which are A or a in proportions p_n, $1 - p_n$ respectively. Then the number X of A genes at time $n + 1$ has the binomial distribution (***), with $n = 2N$, $p = p_n$. It can be shown that the average fraction of A genes at time n is just the proportion p_0 in the first generation. We conclude that *on average*, the A gene frequency remains constant, in agreement with the Hardy-Weinberg Law. However, this situation is very deceptive. It turns out that in fact the proportions of A genes *must* ultimately be 0 or 1, so that the

population eventually comprises either all *A* genes or all *a* genes. Genetic variation is consequently lost!

The phenomenon of loss of variation due to finite population size is known as *random genetic drift*. Clearly, it is possible to sample a population of size $2N$ genes which contains no *A* genes, in the same way that our series of coin-flips could result in no heads.

CONCLUSIONS

In this article, we have presented some of the genetic models that are used to describe the genetic composition of populations. The precise nature of the interplay between selection, mutation and random drift is still under active research.

REFERENCES

[1] *Biological Science: the Web of Life*. Australian Academy of Science, Chapter 34.

[2] Ewens, W.J. (1969). *Population Genetics*, Methuen, London.

[3] Hardy, G.H. (1908). Mendelian proportions in a mixed population. *Science*, Vol.28, pp.49-50.

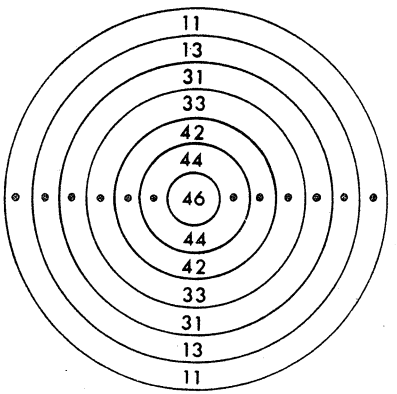
[4] Weinberg, W. (1908). Über den Nachweis der Vererbung beim Menschen. *J. Ver. Vaterl. Naturk. Württemb.*, Vol.64, pp.368-382.

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞

PROBLEM SECTION

PROBLEM 4.5.1.

What is the minimum number of hits necessary to score exactly 100 on this rather unusual rifle target? (This is like the "knapsack" problem mentioned in J. Stillwell's article in *Function* 4, Part 3.)



PROBLEM 4.5.2.

In how many ways can LUCKY DIPS be spelt in the following figure?

L	U	C	K	Y
U	C	K	Y	D
C	K	Y	D	I
K	Y	D	I	P
Y	D	I	P	S

PROBLEM 4.5.3.

Show that if a set S of 10 different numbers is chosen from 1,2,3,...,98,99, there will always be two completely disjoint subsets of S whose sum is the same. For instance, if $S = \{1,18,20,22,33,49,57,58,83,87\}$, then $22 + 49 = 18 + 20 + 33$. This time, it happens that $1 + 57 = 58$, too.

MORE ON PROBLEM 4.1.2.

We partly solved this problem in *Function* Vol.4, Part 3. Andrew Johnston of Ignatius Park College, Townsville, has submitted a solution to the remaining part of the problem: "Is it possible to find six different positive numbers such that each is the product of two of the others?" Andrew found an infinite number of solutions. Let m and n be any two different positive real numbers. Then the set $\{m,n,\frac{1}{n},\frac{1}{m},\frac{n}{m},\frac{m}{n}\}$ can consist of six different positive numbers (with a few special provisos, e.g. $n \neq \frac{1}{m}$) and each is the product of two others:

$$m = \frac{m}{n} \times n \qquad \frac{n}{m} = n \times \frac{1}{m}$$

$$n = \frac{n}{m} \times m \qquad \frac{m}{n} = m \times \frac{1}{n}$$

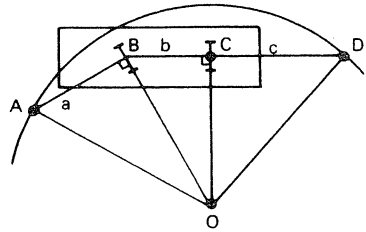
$$\frac{1}{m} = \frac{n}{m} \times \frac{1}{n} \qquad \frac{1}{n} = \frac{m}{n} \times \frac{1}{m}$$

SOLUTION TO PROBLEM 4.2.4.

Baggage trains used at airports, railway stations, etc. have a small tractor which pulls a train of 4-wheeled trailers, each connected to the one in front. The back axle of each trailer is fixed, and the front axle pivots, being steered by the towing bar connecting the trailer to the one in front. An underneath view of a trailer is shown overleaf.

Problem: how should the dimensions a, b and c be proportioned so as to make the train follow as nearly as possible the path taken by the tractor?

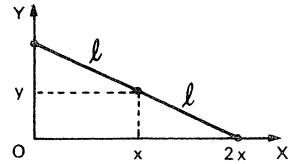
A main requirement of such a train would be for it to travel well around a circular arc. The wheels would need to travel parallel to the circle (i.e. perpendicular to its radii), and the front and rear fittings (the loop A and hook D) would need to travel in the *same* circle and at the same radius. In the diagram, we need $OA = OD$, that is $OA^2 = OD^2$. Using right angle triangles, this reads $a^2 + OB^2 = OC^2 + c^2$ that is $a^2 + b^2 + OC^2 = OC^2 + c^2$, and thus, finally, we need $a^2 + b^2 = c^2$.



SOLUTION TO PROBLEM 4.3.2.

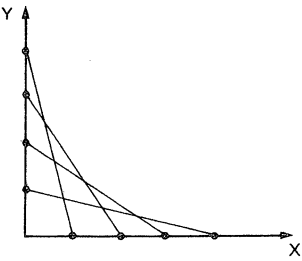
(iii) The mid-point of a ladder sliding down a wall does *not* trace out an asteroid. What *is* the curve?

If the ladder is of length 2ℓ, and the foot is at position $2x$, then the mid-point (x,y) is such that $x^2 + y^2 = \ell^2$, so that it travels along a quarter-circular path.



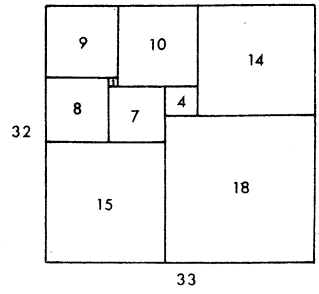
(iv) What curve is obtained by joining equally spaced points along the x and y axes?

The lines here are tangents to a parabola, as discussed in the article by P. Greetham on Curve-Stitching, *Function* Vol.4, Part 3.



SOLUTION TO PROBLEM 4.4.4.

Squares of sides 1, 4, 7, 8, 9, 10, 14, 15 and 18 can be arranged to form a rectangle of sides 32 and 33 as in the diagram.



THE LESSON

THE TEACHER: Listen to me, Mademoiselle, if you do not learn to understand deeply these principles, these fundamental ideas of arithmetic, you will never learn to carry out properly the work of an engineer. ... I recognise that it is not easy, that it is very, very abstract - evidently - but how can you, without deeply understanding the first principles, learn to calculate in your head, and this is the least that would be required of an average engineer, for example, 3 755 998 251 times 5 162 303 508.

THE PUPIL (*very quickly*): 19 390 002 844 219 164 508.

THE TEACHER (*astonished*): No. I think not. It should be 19 390 002 844 219 164 509.

THE PUPIL: No. 508.

THE TEACHER (*more and more astonished, calculates in his head*): Yes, you are right. The product is correct. (*He mutters unintelligibly*) ... quintillions, quadrillions, trillions, billions, millions ... (*Distinctly*) one hundred and sixty four thousand five hundred and eight ... (*Stupefied*) But how could you do it if you do not understand the underlying principles of arithmetic?

THE PUPIL: It's simple. Not trusting my powers of reasoning I learnt by heart all possible results of all possible multiplications.

THE TEACHER: That's rather difficult ... However, permit me to say that that does not satisfy me, Mademoiselle; I do not congratulate you: in mathematics and especially in arithmetic what counts - because in arithmetic it is always necessary to count - what counts above all is understanding. It is by mathematical reasoning, inductive and deductive at the same time, that you must find this answer, and also all other results. Mathematics is the bitter enemy of memory, excellent elsewhere, but wholly harmful in arithmetic. I am therefore not happy ... you are not getting on well at all.

THE PUPIL (*desolated*): No, sir.

translated from "La leçon" by
Eugène Ionesco (written June 1950,
first produced at the Théâtre de Poche,
20 February, 1951).

[Note by translator [G.B.P.]. Both products given in the above extract are wrong. The correct answer is

19 389 602 947 179 164 508.]

∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞ ∞