216

[redacted]

Cours/Lecture Series

1988-1989 ACADEMIC TRAINING PROGRAMME

SPEAKER : R. F. CHURCHHOUSE / Department of Computing Mathematics,
University of Wales, College of Cardiff

TITLES : Major mathematical achievements of recent years
Fractals

DATES : 22, 23 & 24 May
25 & 26 May

TIME : 11.00 to 12.00 hrs

PLACE : Auditorium

ABSTRACT

Major mathematical achievements of recent years (22 to 24 May)

In recent years a number of long-standing conjectures in various branches of mathematics including Number Theory, Graph Theory, Analysis and Group Theory have been proved or disproved and, in addition, significant advances have been made towards the solution of a number of other outstanding problems. In these lectures, which are intended for non-specialists, the history of these conjectures and problems will be given and the methods leading to their complete or partial solution will be summarized. Specific problems to be considered include the representation of irrationals by rationals, transcendence, the Mertens Conjecture, Fermat's Last Theorem and the Euler Generalisation and the Four Colour Theorem.

Fractals (25 & 26 May)

Although the concept and construction of curves, surfaces and solids of fractional dimension goes back almost 100 years it is only since the work of Mandelbrot (1975) illustrated through the medium of high quality computer graphics that the extraordinary complexity and diversity of fractals has been revealed. The lectures will be concerned with the theory, generation and various aspects of fractals.

24/2374

Lecture Notes Distribution : - internal (CERN) distribution only to Participants
- self-service (50 copies) at CERN Main Library

- No extra copies available
- Reference copy at Main Library

CERN Academic Training Programme
May 22nd - 26th 1989

RECOMMENDED BOOKS/Articles

Recent Advances In Mathematics

Two very readable recent books which give, *inter alia*, very good surveys of the topics covered in the lectures for non-specialists are:

(1) Keith Devlin: "Mathematics : The New Golden Age" Pelican, London (1988).

(2) Philip J.Davis and Reuben Hersh: "The Mathematical Experience", Pelican, London (1986).

These books also provide references to more specialised articles and books as well as to original papers.

For the 4-colour problem:

Kenneth Appel and Wolfgang Haken: "The solution of the four-colour map problem ", Scientific American, Vol. 237 (Oct. 1977), 108-21 -

this was the first 'popular' account by the pair who proved the theorem.

Fractals: Three books which cannot be recommended too highly both for technical content and an aesthetic treat:

1. B.B.Mandelbrot: "The Fractal Geometry of Nature", W.H.Freeman & Co., New York, (1982).
2. H-O Peitgen and P.H.Richter: "The Beauty of Fractals", Springer-Verlag, New York, (1986).
3. H-O Peitgen and Dietmar Saupe (Eds.) "The Science of Fractal Images", Springer-Verlag, New York (1988).

These books contain many references to original papers.

R.F.Churchhouse.

Preliminary remarks, definitions

In these lectures when we speak of a polynomial of degree n

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots a_o$$

we assume that all the coefficients (a_n, a_{n-1}, .. a_o) are integers and $a_n \neq 0$.

Definition θ is said to be *an algebraic number of degree n* if it is a root of a polynomial of degree n but is not a root of any polynomial of degree less than *n*.

A *rational* number is an algebraic number of degree 1, i.e. is of the form $\frac{p}{q}$ where p and q are integers.

An algebraic number of degree 2 or higher is said to be an *irrational algebraic number.*

If a number is not a root of a polynomial of any finite degree it is said to be *transcendental.*

Whereas the existence of irrational algebraic numbers is easily proved (Euclid proved that $\sqrt{2}$ is irrational) it is not obvious that transcendental numbers exist and a proof that any given number (such as π or e) is transcendental is never easy. Even proving the *irrationality* of any given number may involve great ingenuity; it is not known for example whether

$$e + \pi$$

is irrational, let alone transcendental.

A basic reason why problems of transcendence are difficult is that, whereas if θ, ∅ are *algebraic* numbers so are

$$\theta + \emptyset,\ \theta - \emptyset,\ \theta\emptyset \text{ and } \theta/\emptyset$$

it is not always true that the sum, difference, product or quotient of two *transcendental* numbers is transcendental

E.g. if π is transcendental (it is) then so is $(4-\pi)$

but $\pi + (4-\pi) = 4$

is algebraic.

LECTURE 1

RATIONAL APPROXIMATION TO IRRATIONALS

RATIONAL APPROXIMATION TO IRRATIONALS

Problem If θ is an irrational number how can we find 'good' rational approximations p/q to θ, and how 'good' are they likely to be?

e.g. $\pi \doteqdot 3.14159265$

$$\frac{22}{7} \doteqdot 3.14285714$$

so $\left|\pi - \frac{22}{7}\right| \doteqdot 1.3 \times 10^{-3}$

Also $\frac{355}{113} \doteqdot 3.14159292$

so $\left|\pi - \frac{355}{113}\right| \doteqdot 3 \times 10^{-7}$

The second approximation is much better but it involves larger integers (355, 113) than the first (22,7).

It can be proved that given any irrational number, θ, we can find an infinity of rationals

$$p_1/q_1, p_2/q_2, \ldots, p_n/q_n, \ldots$$

such that if p/q is any one of them

$$|\theta-\frac{p}{q}| \le \frac{1}{q^2\sqrt{5}}$$

and the proof is "effective" since it shows that these rationals can be found from the continued fraction for θ.

The theorem is "best possible" in the sense that it holds with equality when

$$\theta = \frac{1}{2}(\sqrt{5}-1)$$

<u>Continued fractions</u> These are found by a simple algorithm which involves only the recursive application of

(i) finding the difference between θ and its integer part,

(ii) replacing θ by the reciprocal of this difference.

<u>Example</u>

$$\pi = 3.14159265\ldots$$

$$= 3+0.14159265\ldots$$

$$= 3+\frac{1}{7.0625133\ldots}$$

$$= 3+\frac{1}{7+.0625133\ldots}$$

To save space we then write

$$\pi = 3 + \frac{1}{7+}\;\frac{1}{15+}\;\frac{1}{1+}\;\frac{1}{292+}\ldots$$

The "good" approximations are found by evaluating this expression, as a fraction, after 1,2,3,... terms

$$\pi = \frac{3}{1}, \frac{22}{7}, \frac{333}{106}, \frac{355}{113}, \ldots$$

Some numbers have continued fractions which show a pattern, in particular numbers which are quadratic irrationals have periodic c.f expansions e.g.

$$\sqrt{2} = 1 + \frac{1}{2+}\ \frac{1}{2+}\ \frac{1}{2+\dots.}$$

which leads to the convergents ("good approximations")

$$\frac{1}{1}\ ,\ \frac{3}{2}\ ,\ \frac{7}{5},\ \frac{17}{12},\ \frac{41}{29},\ \dots$$

The number e, which is transcendental (i.e. not the root of a polynomial of any degree), also shows a pattern

$$e=2+\frac{1}{1+}\ \frac{1}{2+}\ \frac{1}{1+}\ \frac{1}{1+}\ \frac{1}{4+}\ \frac{1}{1+}\ \frac{1}{1+}\ \frac{1}{6+..-}$$

the pattern (2n,1,1) extending to infinity. π shows no pattern nor do any known algebraic numbers of degree ≥ 3 (such as $2^{1/3}$).

LIMITS TO THE ACCURACY OF THE APPROXIMATIONS

We know how to find an infinity of pairs of integers (p,q) such that

$$\left|\theta - \frac{p}{q}\right| \leq \frac{1}{q^2\sqrt{5}}$$

- but can we do better than this?

Unless θ is related to $\frac{1}{2}(\sqrt{5}+1)$ we can replace $\sqrt{5}$ by $\sqrt{8}$ (and unless .....) but there is a fundamental limit when θ is an algebraic number of degree n given by

Theorem (Liouville, 1844) If θ is an algebraic number of degree n there exists a constant c, which depends only on θ, such that for all integers p, q

$$\left|\theta - \frac{p}{q}\right| > \frac{c}{q^n}$$

Transcendental Numbers

The existence of transcendental numbers follows from Liouville's Theorem (and also from Cantor's Theory of Enumerability) but proving that any particular number such as

$$e, \pi \text{ or } \log 2$$

is transcendental (or not) is extremely difficult:

In 1873 Hermite proved that

e is transcendental

In 1882 Lindemann generalised this and proved that

"If x is algebraic (and not=0) then

e^{x} is transcendental"

It follows from this that:

π is trancendental

(for $e^{2\pi i} = 1$ and if π is algebraic so is $2\pi i$, but this contradicts Lindemann's theorem).

From Liouville's Theorem it not only follows that transcendental numbers exist it also enables us to construct some e.g.

$$\theta = \sum_{n=0}^{\infty} 2^{-(n!)}$$

It was not believed that Liouville's Theorem was the best possible result but it was more than 60 years before an improved form of it was established. What was sought was a theorem of the type

"If θ is an algebraic number of degree n there are only finitely many pairs of integers (p,q) such that

$$\left|\theta - \frac{p}{q}\right| < \frac{1}{q^k} \text{ "}$$

Liouville's theorem shows that this is true when k > n and false when k = 2.

The great problem was: what, in the interval (2,n) is the true value of k?

Closing the gap

In 1909 Thue proved:

"For $n \geq 3$ we can take $k = \frac{1}{2}n + 1$"

In 1921 Siegel improved this to:

"For $n \geq 2$ we can take $k = 2\sqrt{n}$"

In 1947 Dyson further improved this to:

"For $n \geq 2$ we can take $k = \sqrt{2n}$"

Then, in 1955, K.F.Roth achieved the ultimate:
For $n \geq 2$ we can take $k = 2+h$ where h is arbitrarily small"

- the gap was completely closed (and Roth got the 1956 Fields Medal).

THE GELFOND-SCHNEIDER THEOREM

No really general theorems relating to transcendence were proved until 1929 when Gelfond proved a particular version of a theorem which was generalised by himself and Schneider independently in 1934.

Theorem (Gelfond-Schneider, 1934) If a and b are algebraic numbers, $a \neq 0$ or 1 and b is irrational then a^b is transcendental.

This remarkable theorem solves, as a very special case, Hilbert's 7th Problem (1900):

Is $2^{\sqrt{2}}$ transcendental? (It is). Even more spectacularly:

Theorem: e^π is transcendental
(Proof; put a = i, b = -2i in the Gelfond-Schneider theorem).

At the other extreme however we cannot even prove that $e+\pi$ is irrational, let alone transcendental (similarly $e-\pi$ etc).

RECENT DEVELOPMENTS

Both Roth's Theorem and the Gelfond-Schneider Theorem have been generalised in recent years, by Schmidt and Baker respectively.

Roth's theorem deals with approximations to algebraic irrationals by rationals. In 1970 Schmidt generalised this to approximation to algebraic irrationals by algebraic numbers of lower degree:

Theorem (Schmidt, 1970) If a is an algebraic number of degree > n and h is any number >0 there are only finitely many algebraic numbers b of degree ≤ n such that

$$|a-b| < c^{-(n+1+h)}$$

where c is the largest absolute value of the coefficients of the polynomial satisfied by b.

Roth's Theorem is the special case n=1 and the theorem tells us, for example, that a cube root cannot be approximated by quadratic irrationals more closely than (effectively)

$$c^{-3}.$$

BAKER'S generalisation of the Gelfond-Schneider Theorem

The Gelfond-Schneider Theorem can be stated in various ways including:

Theorem If a_1, a_2, b_1 and b_2 are any non-zero algebraic numbers such that $\log a_1$, $\log a_2$ are linearly independent over the rationals then

$$b_1 \log a_1 + b_2 \log a_2 \ddagger 0.$$

This was generalised by Baker:

Theorem (Baker, 1966) If a_1, a_2, ..., a_n are non-zero algebraic numbers such that $\log a_1$, $\log a_2$..., $\log a_n$ are linearly independent over the rationals then

$$1, \log a_1, \log a_2, ..., \log a_n$$

are linearly independent over all algebraic numbers.

(Baker was awarded the 1970 Fields Medal for this result).

Unsolved Problems

Questions of irrationality and transcendence are among the most difficult in mathematics. Among the many unsolved problems are:

(1) Euler's constant y (=0.577...) is defined by

$$y = ;\lim_{n\to\infty} (1+\underline{1} + \underline{1} + .. \underline{1}) - \log e^{n}$$

Is y irrational?

(2) It is known that

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + ... = \frac{\pi^2}{6}$$

and $$1 + \frac{1}{2^4} + \frac{1}{3^4}\, t\, .. = \frac{\pi^4}{90} \text{ etc}$$

so these numbers are not only irrational but are transcendental; however only recently has it been proved that

$1 + \frac{1}{2^3} + \frac{1}{3^3} + ...$ is irrational; is it transcendental?

As for $1 + \frac{1}{2^5} + \frac{1}{3^5} + ...$, is it irrational?

(3) Continued fractions of algebraic numbers of degree 3

Algebraic numbers of degree 2 have periodic continued fractions so the elements ("partial quotients") of their continued fractions are bounded.

Are the partial quotients of algebraic numbers of degree 3 bounded or not?

(The statistical evidence suggests that the answer is "No", but the sample studied is not large and it is not impossible that the partial quotients are bounded but not according to any simple formula).

LECTURE 2

DIOPHANTINE EQUATIONS

HILBERTS TENTH PROBLEM

(with a brief introduction to

Algebraic Number Fields)

Algebraic Number Fields

If θ is an algebraic number of degree n then numbers of the form

$$m_0 + m_1\theta + m_2\theta^2 + \ldots\ldots + m_{n-1}\theta^{n-1}$$

where $m_0, m_1, \ldots, m_{n-1}$ are rational numbers form a field under the operations of +,-,x and ÷

These fields have elements which can be classed as (algebraic) integers e.g. those elements which satisfy a polynomial (of degree $\leq$ n) with leading coefficient equal to one.

The fields also have elements which are "units", divisors of 1, and there may be a finite or infinite number of these e.g.

(1) in the "Gaussian" field where $\theta = i$ the units are i, -i, 1 and -1 and are all generated by powers of i ("the fundamental unit");

(ii) in the field where $\theta = \sqrt{2}$ there are an infinity of units generated by all integer powers (positive, zero, negative)
of the fundamental unit $(\sqrt{2}+1)$ (Note that $(\sqrt{2}+1)$ $(\sqrt{2}-1) = 1$).

These fields also have primes, integers which have no integer divisors other than themselves and units. The 'ordinary' primes are not necessarily primes in algebraic number fields

e.g. $5 = (2+i)(2-i)$

and $2 = (1+i)(1-i)$

are not primes in the Gaussian Field, whereas 3 and 7 are.

Unique factorisation does not hold in general in algebraic number fields e.g. $6 = 2 \times 3 = (1+\sqrt{-5})$ $(1-\sqrt{-5})$

but 2, 3, $1 \pm \sqrt{-5}$ are all <u>primes</u> in this field.

The field based on $\sqrt{-5}$ is the 'first' where unique factorisation fails.

For further reading consult books on

Algebraic Number Theory.

DIOPHANTINE EQUATIONS

These are equations in one or more variables where we seek a solution in integers.

Such equations may have no solutions, one, many or an infinity.

E.G. $x^2+1 = 0$ (NO SOLUTION)

$2x+7 = 15$ ($x=4$)

$x^2+y^2 = z^2$ (an infinity of solutions given by $x = a^2-b^2$, $y=2ab$, $z = a^2+b^2$)

Given any particular Diophantine Equation we are usually faced with the problem of either finding a solution or proving that no solution exists.

For example it is easy to prove that

$$x^3+y^3+z^3 = 4$$

has no solutions but, despite extensive searches no solution of

$$x^3 + y^3+ z^3 = 30$$

has been found but neither has it been proved that none exist.

HILBERT'S TENTH PROBLEM

In 1900 David Hilbert listed 23 major unsolved problems of mathematics, the solution of any of which would significantly advance mathematical knowledge.

The tenth problem was:

Given a Diophantine Equation in any number of unknowns and with integral coefficients to devise a process by means of which we can determine in a finite number of operations whether the equation is solvable in integers or not.

In 1970 Yuri Matyasevich (aged 22) building upon results proved between 1950 and 1970 by Martin Davis, Julia Robinson and Hilary Putnam proved that no such process (i.e. algorithm) exists.

The proof lies in the area of mathematical logic and computability (i.e. Turing machines).

COMPUTABLE SETS

A set of integers S is said to be computable if there exists a Turing machine program which, given any integer N as input, halts with an output 1 if N is a member of S and halts with an output of 0 if N is not a member of S.

Note that the possibility that the Turing machine never halts is here excluded, but is allowed in:

Recursively Enumerable Sets

A set of integers S is said to recursively enumerable if there exists a Turing machine program which, given any integer N as input, halts with an output 1 if N is a member of S and otherwise either halts with an output 0 or does not halt at all.

STEPS IN THE SOLUTION OF HILBERT'S TENTH PROBLEM

Davis (1950) tried to show that for every recursively enumerable set, S, there exists a polynomial

$$p_s(x, y_1, y_2, \dots y_n)$$

with integer coefficients with the property that a positive integer N belongs to S if and only if the Diophantine Equation

$$p_s(N,y_1,y_2,\dots, y_n) = 0$$

has a solution.

If this were so then by choosing s to be a non-computable set it would follow that no such algorithm of the type sought by Hilbert can exist for if it did we would know whether the associated Diophantine Equation has a solution so that s would be computable, which is a contradiction.

Davies was unable however to prove that such a polynomial always exists.

ROBINSON (1960) collaborated wit Davis and Putnam to show that just one Diophantine could be foun whose solutions grow exponentiall then it would be possible to find Diophantine Equation for ever recursively-enumerable set and s solve Hilbert's Tenth Problem.

Matyasevich (1970) constructed Diophantine Equation in 14 variable and terms of degree 4 based upon th elements of the Fibonacci Series

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ..

the terms of which grow exponentially since the n-th term asymptotically approaches

$$\frac{1}{\sqrt{5}}\left(\frac{1}{2}(1+\sqrt{5})\right)^n$$

The existence of this equation combined with the Davis-Robinson-Putnam resul solves Hilbert's Tenth Problem.

MATYASEVICH'S DIOPHANTINE EQUATION

In the 10 polynomial equations below v and u are related in such away that v is the 2u-th Fibonacci Number.

Square each of the 10 equations and add them togeher to produce a single Diophantine Equation of degree 4 in 14 variables. This equation settled Hilbert's Tenth Problem.

$$
\begin{aligned}
u + w - v - 2 &= 0, \\
l - 2v - 2a - 1 &= 0, \\
l^2 - lz - z^2 - 1 &= 0, \\
g - bl^2 &= 0, \\
g^2 - gh - h^2 - 1 &= 0, \\
m - c(2h + g) - 3 &= 0, \\
m - fl - 2 &= 0, \\
x^2 - mxy + y^2 - 1 &= 0, \\
(d - 1)l + u - x - 1 &= 0, \\
x - v - (2h + g)(l - 1) &= 0.
\end{aligned}
$$

A PRIME-GENERATING POLYNOMIAL

For many centuries the question as to whether there exists a polynomial which takes only prime values when its variables are integers has been unresolved. It can be proved that no polynomial in a single variable can have such a property although some, such as

$$n^2 - 79n + 1601$$

which is prime for $0 \leq n \leq 79$

do remarkably well.

It is however a consequence of the method of disproof of Hilbert's Tenth Problem that there must be a Diophantine Equation which describes the primes which implies that there must be a polynomial whose <u>positive</u> values (as its variables range over all the integers) are the primes - but its negative values may or may not be negative primes).

Finding such a polynomial is a different matter but in 1977 one was found by Jones, Sato, Wada and Wiens; it is of degree 25 and involves 26 variables.

THE PRIME GENERATING POLYNOMIAL OF JONES, SATO, WADA AND WIENS

This was found in 1977; it involves 26 variables and is of degree 25 and is:

$$
\begin{aligned}
&(k + 2)\{1 - [wz + h + j - q]^2 \\
&\quad - [(gk + 2g + k + 1)(h + j) + h - z]^2 \\
&\quad - [2n + p + q + z - e]^2 \\
&\quad - [16(k + 1)^3(k + 2)(n + 1)^2 + 1 - f^2]^2 \\
&\quad - [e^3(e + 2)(a + 1)^2 + 1 - o^2]^2 \\
&\quad - [(a^2 - 1)y^2 + 1 - x^2]^2 - [16r^2y^4(a^2 - 1) + 1 - u^2]^2 \\
&\quad - [((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 \\
&\quad - [n + l + v - y]^2 - [(a^2 - 1)l^2 + 1 - m^2]^2 \\
&\quad - [ai + k + 1 - l - i]^2 \\
&\quad - [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 \\
&\quad - [q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 \\
&\quad - [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2\}.
\end{aligned}
$$

FERM^T"S 'LAST THEOREM'

The Diophantine Equation

$$x^n + y^n = z^n$$

is the most notorious one of all. It has an infinity of solutions when n=1 or 2.

In 1639 Fermat claimed that he had a "truly marvellous" proof that it had no solutions (other than the trivial one where xyz=0) when $n \geq 3$. He never published the proof and none has been found to this day.

Hundreds of false"proofs" have been produced and it is highly probable that Fermat's proof contained a flaw: he might have assumed, as many others have done, that unique factorisation holds in algebraic number fields, but it was only in 1844 that Kummer realised that this is not always the case

e.g. $6 = 2 \times 3 = (1+\sqrt{5})\ (1-\sqrt{-5})$

- so unique factorisation does not hold in the algebraic number field based on $\sqrt{-5}$.

Kummer's attempted proof was valid for the 7 odd prime values $n \leq 19$ (where the related algebraic number fields do possess unique factorisation)

[It is only necessary to prove the theorem in the cases where n is an odd prime or $n=4$; the case $n=4$ is fairly easily proved].

By introducing the concept of "ideals" Kummer was able to extend his proof to cover all odd primes ≤ 100 with the exception of 37, 59 and 67; but he also proved much more

An unexpected twist : the Bernoulli Numbers

The Bernoulli Numbers, B_n, are defined by a power series viz.

$$\frac{x}{e^x-1} = 1+B_1\frac{x}{1} + B_2\frac{x^2}{2!} + B_3\frac{x^3}{3!} + ..$$

so that

$B_1={}^1/_2$, $B_2={}^1/_6$, $B_3=0$, $B_4={}^-1/_{30}$, ...

ALTHOUGH THE BERNOULLI NUMBERS ARE INITIALLY QUITE SMALL THEY EVENTUALLY BECOME LARGE

e.g. $B_{16} = -3617/510$

and $B_{34} = 2577687858367/6$

There would not appear to be the slightest connection between the Bernoulli Numbers and Fermat's Last Theorem, but there is.

A prime p is said to be regular if it does not divide any of the numerators of $B_2, B_4, \ldots, B_4, \ldots, B_{p-3}$.

In 1847 Kummer proved that Fermat's Last Theorem is certainly true for all regular primes p. Of the primes below 100 only 37, 59 and 67 are irregular (hence the result above).

Now $|B_{2n}|$ grows very rapidly and checking for divisibility by p by hand is very laborious but Kummer did it for all primes up to 163 and found that only eight are irregular.

With the coming of des' calculators and computers the range of application was widely extended and by 1976 all regular primes less than 125,000 had been found.

However only about 60% of primes are regular so what about the 40% or so which are not covered by Kummer's Theorem?

The Bernoulli numbers provide a specific test which provides an assurance that Fermat's Conjecture is true for certain primes, but there are other, more complex, tests that can also be used to cover primes that do not satisfy the first test.

Combining these various tests it has been proved that Fermat's Conjecture is certainly true for all primes < 125,000.

CASE 1 and CASE 2 OF THE FERMAT CONJECTURE

A different line of attack on Fermat's Conjecture distinguishes two cases:

Case 1: If $x^p + y^p = z^p$ then one of x,y,z is divisible by p.

Case 2: None of x,y,z is divisible by p.

Case 1 is more amenable to atack and by 1982 Lehmer had shown that Fermat's Conjecture is true for Case 1 for all primes up to 6×10^9.

It can also be shown that the Case 1 result holds when p is a Mersenne prime viz:

$$p = 2^q - 1$$

where q is itself a prime and so in particular holds for the largest known prime

$$2^{216091} - 1$$

(found by Slowinski using a Cray X-MP in 1985).

These Case 1 results all follow from a criterion discovered by Sophie Germain in 1832 and subsequently extended by Legendre viz

If p is a prime and if any of the numbers

2p+1, 4p+1, 8p+1, 10p+1, 14p+1, 16p+1

is also a prime then Fermat's Last Theorem is true for Case 1 for p.

In 1985 Adleman, Fouvry and Heath-Brown generalised the Germain criterion further and proved that

Case 1 of Fermat's Last Theorem holds for infinitely many primes.

This is the only theorem so far proved in relation to the Fermat Conjecture that applies to an infinity of cases not having a solution. However since we have no such result concerning Case 2 we still do not know if the Fermat Conjecture is true for an infinity of cases or not.

Falting's Theorem

In 1983 Gerd Faltings, a 29-yea old West German, proved the mos important theorem in the history o the Fermat Conjecture:

The Diophantine Equation

$$x^n + y^n = z^n$$

has at most a finite number o primitive solutions for $n \geq 3$.

("Primitive Solutions" means tha x,y,z have no common factor).

Faltings was awarded a 198 Field's Medal for this result.

The Falting's result is importan in a more general context. In 192 Mordell put forward a conjectur that any irreducible polynomial i two variables of genus greater tha or equal to 2 has at most a finit number of rational solutions; this i still unproved but Falting's theoren is a special case - divide throughou by z^n and the equation becomes

$$u^n + v^n = 1$$

where u, v are now rational.

FERMAT'S LAST THEOREM

SUMMARY

$$x^n + y^n = z^n$$

has no solutions in integers if

$$3 \leq n \leq 125{,}000$$

or if

$n=p$, x, y, or z is divisible by p and

$$p < 6 \times 10^9$$

(and this case holds for an infinity of values of $p > 6 \times 10^9$).

Furthermore

The equation has at most a finite number of (primitive) solutions for all $n \geq 3$.

Euler's Generalisation of Fermat's Last Theorem

Euler (c. 1780) generalised the Fermat Conjecture to:

The equation

$$x_1^n + x_2^n + \ldots + x_{n-1}^n = x_n^n$$

has no non-trivial solution in integers when $n \geq 3$.

When $n=3$ the Euler Conjecture is true, since it is the same Fermat's Conjecture.

For $n \geq 4$ no progress was made until 1966 when Lander and Park (Math Comp. 21, 101-103) discovered, with the aid of a CDC 6600 that

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

thus disproving Euler's Conjecture when $n=5$.

In 1987 Elkies found a counter example when $n=4$:

$$(2682440)^4 + (15365639)^4 + (18796760)^4 = (20615673)^4$$

and indeed proved that there are infinity of solutions.

So, for once, Euler got it wrong!

LECTURE 3

THE RIEMANN HYPOTHESIS

MERTEN'S CONJECTURE

and

THE FOUR COLOUR THEOREM

THE RIEMANN HYPOTHESIS AND THE MERTENS CONJECTURE

In the study of the prime numbers the series

$$\zeta(s) = \sum_{n=1}^{\infty} n-s$$

where s=a+ib is a complex number, plays a key role. The reason for this is basically because of the identity, discovered by Euler, that connects a product over the primes with the series over the integers

$$\prod_{p} (1-p^{-s})^{-1} = \sum_{n=1}^{\infty} n^{-s}$$

In 1859 Riemann in the course of a fundamental paper on Prime Numbers remarked that it seemed likely that the series $\zeta(s)$ (it is now known as the Riemann Zeta-Function) had the property that all its zeros have real part (a) equal to 1/2 and that this had important consequences in many problems in Number Theory but that he couldn't prove it.

This is the celebrat d Riemann Hypothesis:
"The complex zeros of ζ (s) all have real part = 1/2"

Despite over a century of effort by hundreds of mathematicians the RH (as it is often written) remains unproved. There is however a lot of evidence that it is true.

In 1914 Hardy proved that

ζ(s) has an infinity of zeros with real part = 1/2

(but there might be some, even an infinity, with real part not = 1/2)

Computation of the zeros began before 1900; the first pair of zeros (they occur in symmetric pairs) are at

$$a = 1/2 + 14.134725i$$

and by 1903 it was shown that all the zeros in the rectangle

$$0 < a < 1, \ -T < b < T$$

lie on the line a = 1/2 when T = 50.

Th range of values of T was steadily exended T = 200 by 1918, 250000 in 1966, 1.2 x IO^8 in 1983 and so far the first 1.5 x 10^9 zeros have been found and all lie on the line $a={}^1/_2$.

So the computational evidence is good, but cases are known where even stronger evidence for a conjecture has proved to be misleading.

There is however support for the RH from another direction, which appears on the surface to be totally unrelated.

The Möbius Function

The Mobius Function μ (n) is defined for positive integers n by

$\mu(1) = 1$
$\mu(n) = (-1)^k$ if n is the product of k distinct primes
$\mu(n) = 0$ if n is divisible by the square of a prime

Thus the sequence of values of μ (n) begins

1, -1, -1, 0, -1, +1, -1, 0, 0, +1

near future.
It is easy to see that the Mobius Function is related to the Riemann Zeta Function by

$$\sum_{n=1} \ (n)n^{-s} = (\ (s))^{-1}$$

Mertens Hypothesis

In 1897 F. Mertens produced a table of values of (n) for n up to 10^4 and included also a table of the cumulative sum

$$M(N) = \sum_{n=1} \ (n)$$

thus the values of (N) begin

1, 0, -1, -1, -2, -1, -2, -2, -2, -1, ..
and he noticed that, up to N = 10^4 at least it was always true that

$$|M| \leq \sqrt{N}$$

and he conjectured that this is always the case; this is the Mertens Hypothesis.

It can be proved that:
If the Mertens Hypothesis is true so is the Riemann Hypothesis, but the Riemann Hypothesis may be true and the Mertens Hypothesis False

A personal conjecture

In 1968 I used Atlas (at what is now RAL) to study (N) for N up to 10^8. My idea was that (n) might behave like a random variable when considered over a large range of values of n, taking the values 0, +1 and -1 as follows

(n) = + 1 with probability $3/\pi^2$

(n) = -1 with probability $3/\pi^2$

(n) = with probability 1 - $6/\pi^2$

(the probability that n is divisible by the square of at least one prime is $1-6/\pi^2$)

Assuming that we can treat (n) as a random variable we would expect that, in any block of 10^6 consecutive integers (n) would be zero about

$$10^6(1-6/\pi^{-2}) = 392{,}073 \text{ times}$$

The table of counts for the first 33 blocks of one million is as shown - the agreement is quite astonishing.

TABLE 2

Million	ν_0	*Million*	ν_0
1	392,074	18	392,088
2	392,049	19	392,039
3	392,104	20	392,037
4	392,037	21	392,072
5	392,103	22	392,084
6	392,076	23	392,096
7	392,053	24	392,047
8	392,101	25	392,096
9	392,061	26	392,071
10	392,051	27	392,071
11	392,073	28	392,065
12	392,078	29	392,079
13	392,073	30	392,065
14	392,095	31	392,083
15	392,083	32	392,077
16	392,093	33	392,076
17	392,057		

TABLE 3

N	ν_0	$E(\nu_0)$	$\nu - E(\nu_0)$
25,000,000	9,801,820	9,801,822.5	− 2.5
50,000,000	19,603,656	19,603,645	+11
75,000,000	29,405,440	29,405,467	−27
100,000,000	39,207,306	39,207,290	+16

(TABLES 2,3 FROM PAPER BY RFC/IJG IN MATH.COMP 22 (1968) 857-862)

The greement between expected and observed values continued right up to $n=10^8$; table 3 shows the situation at 25, 50, 75 and 100 million.

These results strongly suggest that we can regard $\mu(n)$ as a random variable and hence $M(N)$ as a random walk.

I showed these results to I.J.Good, a well-known expert in probability theory, who was at the Atlas Laboratory at that time and he said that the results were so strong that we would be justified in applying the Central Limit Theorem.

We did so and put forward a number of conjectures in consequence, one of which is:

Conjecture (IJG-RFC, 1968)

The upper limit of

$$M(N)\ (N \log \log N)^{-1/2} \text{ is } \sqrt{12}/\pi$$

and pointed out that this implies that

(i) the Mertens Conjecture is false;

(ii) the Riemann Hypothesis is true.

DISPROOF OF THE MERTENS CONJECTURE

There seemed, in truth, to be no obvious reason why the Mertens Conjecture should be true and the evidence of Jack Good and myself indicated that it was probably false. Computer studies were pursued in the hope of finding a value of N such that $M(N)>N^{1/2}$ but the Mertens Conjecture was finally disproved by Odlyzko and te Riele in 1983 by a different method involving the computation of 2000 zeros of the Zeta Function to 100 decimal places which took 40 hours on a Cyber 750 and a further 10 hours on a Cray-1.

The proof shows that there exists an N such that

$$M(N) > 1.06\sqrt{N}$$

but that such an N exceeds 10^{30}, so that a direct search for it is out of the question.

The IJG-RFC Conjecture is strengthened by the disproof of Mertens but, since it implies the truth of the Riemann Hypothesis I doubt if anyone will prove it in the near future.

THE FOUR-COLOUR THEOREM

In 1852 Francis Guthrie (a student) observed that it always seemed to be possible to colour any map drawn on a piece of paper with (at most) 4 colours in such a way that no countries having a common border were coloured the same.

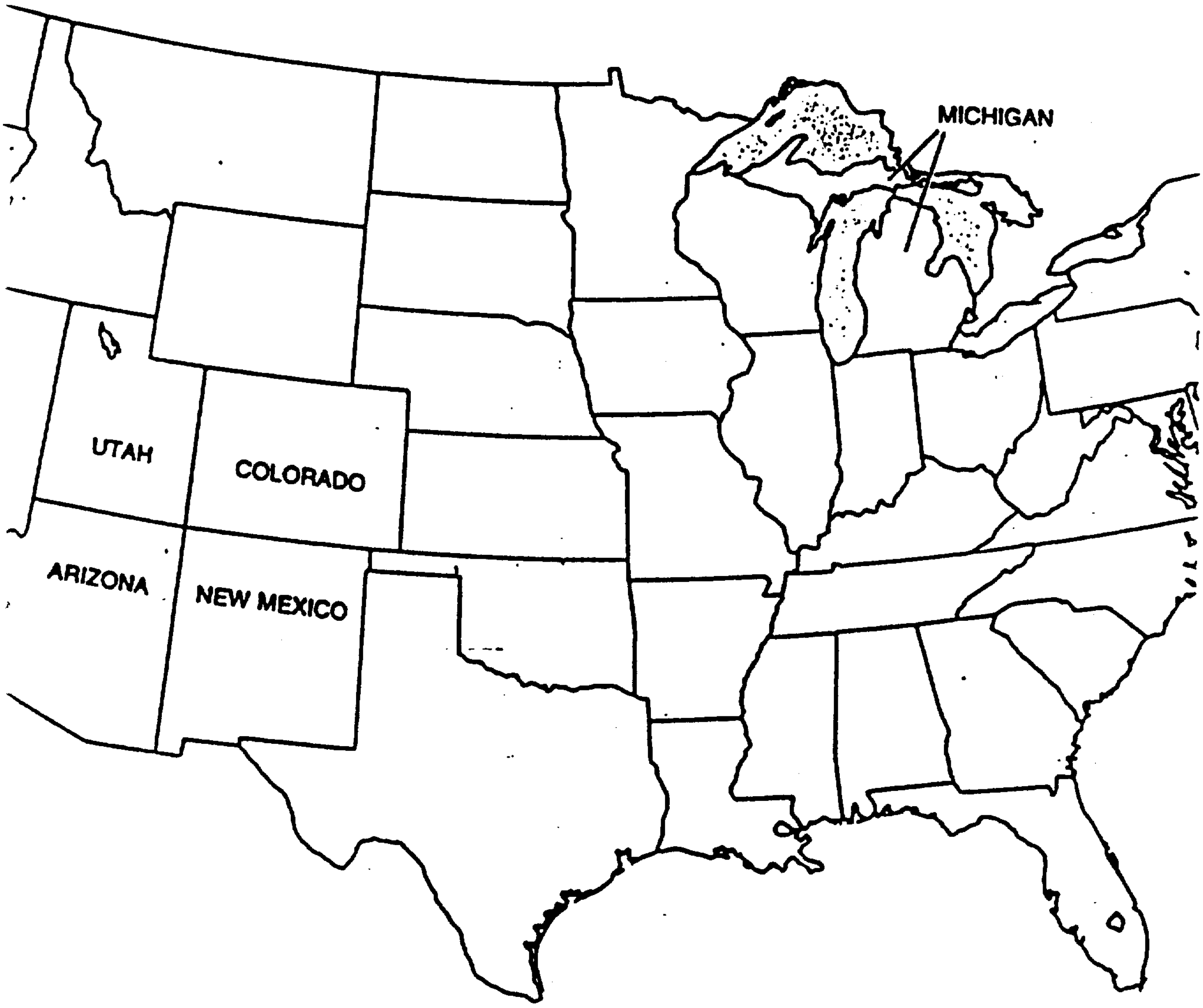
NOTE:

(1) Countries which meet only at a point are not considered to have a common border;

(2) A country is a connected region - regions without a common border are considered distinct;

(3) The (infinite) region which surrounds the entire map is also considered to be a country (or ocean) which must be coloured.

So, in the map of the United States the States of Arizona and Colorado, which meet at a point, are not considered to have a common border, and so may be coloured the same. On the other hand the State of Michigan, which consists of two disconnected regions is to be regarded as 2 different States.



A
a
F
s
a
w
p
tl

Ir
fl
tl
cl
tl
p
H
c

K

N

(i

(ii

A few people, including de Morgan and Cayley attempted to prove the Four Colour Conjecture without success and aroused interest in it and in 1879 A.B.Kempe (a barrister with a mathematical training) published what he, and everyone else, thought was a proof.

In 1890 P.J.Heawood pointed out a flaw in Kempe's proof but, despite this flaw, Kempe deserves great credit for not only was his method the one that ultimately led to the proof, 97 years later, but also Heawood used it to prove that 5 colours are certainly sufficient.

Kempe began by defining

Normal maps are maps in which

(i) no country is entirely enclosed by another country;

(ii) no more than 3 countries meet at any point.

ATTEMPTS TO PROVE HE FOUR-COLOUR THEOREM, 1890-1975

Following the publication of Heawood's paper in 1890 many attempts were made to prove the Four Colour Conjecture and proofs were obtained that if a map required five colours then the map must contain at least a certain number of countries where "a certain number" was steadily increased from 26 (in 1922) to 96 (in 1975).

In 1976 Appel and Haken proved the Four Colour Theorem.

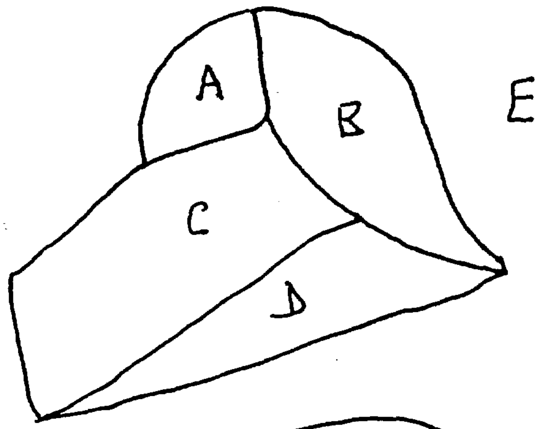
Maps and Graphs The first step in the proof of the Four-Colour Theorem is to convert maps into graphs since graphs contain all the information about maps and the well-developed mathematical theory of graphs can be applied. The actual shape of a country doesn't matter, only which other countries it adjoins. (In other words, it is the topology that matters, not the geometry).

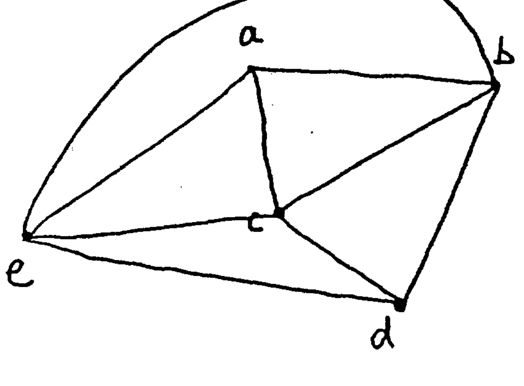
Basically we replace each country by a point (we can think of it as the capital of the country) and join two points if, and only if, their corresponding countries have a common border.

Definition A planar graph is a finite collection of points (called vertices) with some of the points joined by arcs (called edges) with the property that edges do not intersect except at vertices.

When drawn in the plane such a graph breaks the plane up into a number of regions, called faces.

Example of a map and its corresponding graph.





The Graph version of the Four-Colour Conjecture

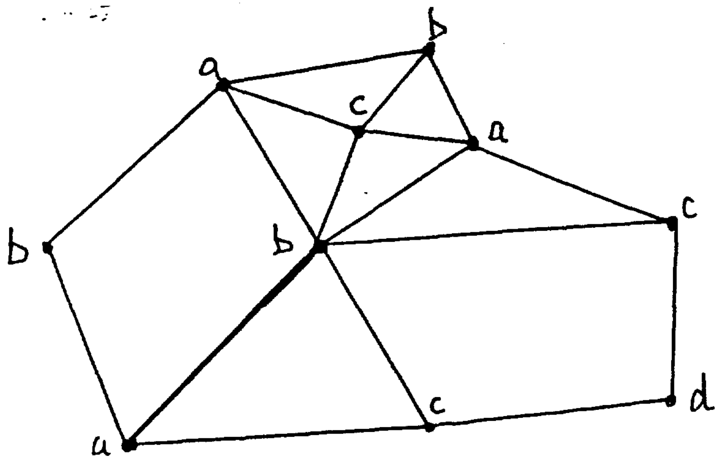
The problem of colouring a map so that no two adjacent countries have the same colour is equivalent to colouring the vertices of a graph so that no two vertices which are joined by an edge are coloured the same.

Euler's Formula

If a planar graph as V vertices, E edges and F faces then V, E, and F are related by a fundamental formula which was discovered by Euler in the 18th century:

$$V - E + F = 2$$

So, for example in the graph below



we have V=10, E=17, F=9 (recall that the outside region counts as a face). A suitable colouring with 4 colours is shown.

Key steps in the proof of the Four Colour Theorem

Step 1 Kempe's approach was to assume that some maps exist which require 5 colours. He proved that among these would be normal maps.

He then concentrated on a normal map with the minimum number of countries which requires 5 colours (there might be more than one such map).

His aim was to show that such a map could be "reduced" to a normal map with even fewer countries but which still required 5 colours. This contradiction would prove the 4 colour theorem.

In practice he considered not maps but their corresponding planar graphs.

Valency of a vertex

The valency of a vertex of a graph is the number of edges which meet at that vertex.

Step 2 An early discovery in the study of the 4-colour conjecture was the fact that:

the 4-colour theorem is true if and only if it is true for graphs in which each vertex has valency 3.

Such graphs are called "3-valent.

Step 3 In any minimal 5-colour graph each face has at least 5 edges.

Step 4 If E and V denote the number of edges and vertices of a 3-valent graph

$$2E = 3V$$

(For every edge joins 2 vertices and at each vertex 3 edges meet).

Step 5 Let p_i denote the number of faces of a graph with exactly i edges, then the total number of edges in the graph when we count in this way is 2E (since every edge gets counted twice) but the number is also

$$2p_2 + 3p_3 + 4p_4 + \ldots = 2E \qquad (2)$$

Step 6 The total number of faces is

$$p_2 + p_3 + p_4 + \ldots \qquad (3)$$

and if we now combine Euler's Formula with (1), (2) and (3) we obtain the very important result that

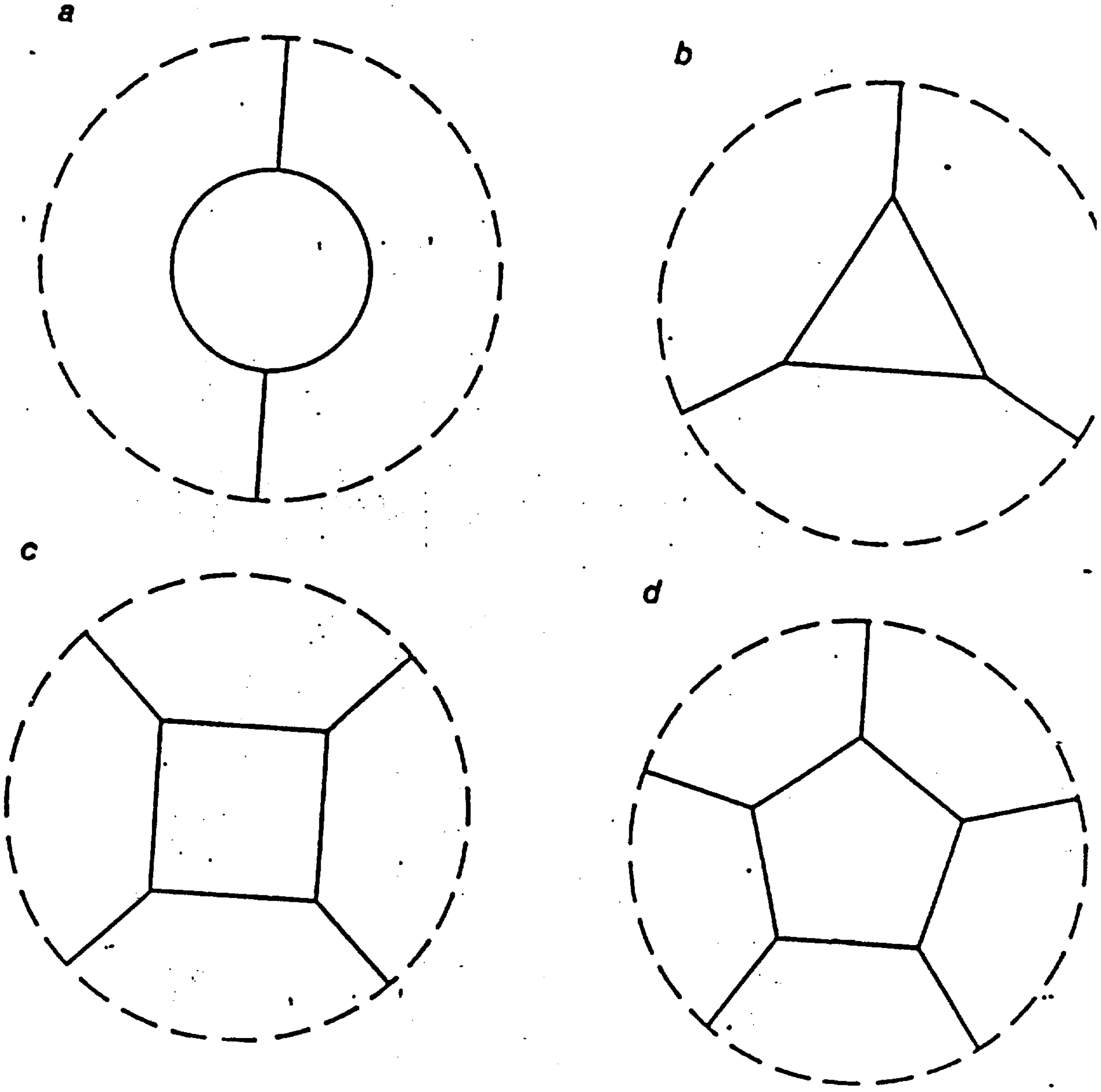
$$4p_2+3p_3+2p_4+p_5-p_7-2p_8\ldots = 12 \qquad (4)$$

STEP 7 It follows fror (4) that at least one of the positive terms on the left must be non-zero hence:

A minimal 5-colour graph has at least one face having no more than 5 edges.

This result was the basis of Kempe's attempted proof and of the successful proof of 1976.

Step 8 Any minimal 5-colour graph must, in consequence of Step 7, have at least one of a number of particular sub-graphs which are shown on the next slide.


a
b
c
d

Step 9

Kempe thought that he had reduced the 4-colour conjecture to the discussion of a relatively small number of cases. Unfortunately it was at this point that he had made his mistake and the number of cases to be considered eventually turned out to be about 1500 (it had been thought that it might be as many as 10000).

The proof of the theorem then required a study of all these cases to show that each of them could be "reduced" to produce a graph with fewer faces.

Appel and Haken began their detailed analysis in 1972 and 4 years later, after 1000 hours of computer time all the cases were finally resolved and the 4-colour theorem was proved.

Variations on the 4-colour theorem

(1) Maps on surfaces which are not planesor spheres

If we have a map on the surface of a torus we find that 4 colours are no longer sufficient to ensure that adjacent countries are not coloured the same and, in fact, we require 7 colours.

Remarkably this result, and an even more general one, was proved by Heawood in 1890. A torus can be regarded as a sphere with one handle and Heawood's result is:

Theorem On a sphere with n handles (where $n \geq 1$) a map can always be coloured with at most

$$\left[\frac{7+\sqrt{1+48n}}{2}\right] \text{ colours,}$$

where [x] denotes the integer part of x.

The proof is invalid when n=0 so, ironically, what would appear to be the simplest case of a general theorem turns out to be the most difficult.

(2) Countries with colonies

If we allow countries to have colonies which must be coloured the same as the parent country we have to consider two cases

(i) the countries and colonies are all on one planet (or surface of a sphere, or plane)

- if no country can have more than one colony it has been proved that 12 colours are both necessary and sufficient;

(ii) when the countries and their colonies are on different planets (such as would happen in the Moon was colonised) it is known that at least 8 colours are necessary and that 12 will suffice, but the exact number which is both necessary and sufficient has not been determined.

Additional References

Rational Approximation to Irrationals and Diophantine Equations

There are many good introductory books on the Theory of Numbers (such as that by G.H.Hardy and E.M.Wright, Oxford Univ. Press, 1977) which cover the more elementary aspects of the topics covered in Lectures 1 and 2.

The Four-Colour Theorem

(i) "The Four Colour Problem" by Thomas L.Saaty and Paul C.Kainen, McGraw-Hill, 1977.

(ii) "Map Coloring, Polyhedra and the Four-Color Problem" by David Barnette, Math.Assoc. of America, 1983.

The Riemann Hypothesis and Mertens Conjecture

There are no elementary books on these topics, though Devlin's book has a very readable account. For those with a good knowledge of Complex Variable Theory:

"The Zeta Function of Riemann" by E.C.Titchmarsh, Oxford Univ.Press, 1951 is a classic.

CERN Academic Training Programme

MAY 22nd - 26th 1989

FRACTALS

The following pages consist of prints of the overhead transparencies and some additional notes given in the two lectures on fractals.

Some references are given at the end.

(The lectures were illustrated by some 30 colour slides, examples of which can be seen in references [2] and [3].)

R.F.Churchhouse

FRACTALS

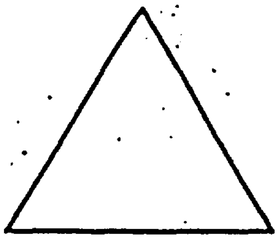
The idea of fractional dimensions has been familiar to mathematicians since the early part of this century, arising from the work of Hausdorff; but it is only relatively recently, beginning with the work of Mandelbrot that fractional dimensions have been shown to be relevant to several branches of science and technology including geography, microbiology and turbulent flow in hydrodynamics.

A common feature of curves of fractional dimension, whether they have a natural or purely mathematical basis, is self-similarity : no matter how small a section of the curve is studied it contains all the features of the whole curve. In nature, coastlines have this property approximately and we can construct such a curve mathematically quite easily, as follows.

We begin with an equilateral triangle with unit sides (Figure 1), clearly the length of its perimeter is 3 units.

We begin with an equilateral triangle with unit sides (Figure 1), clearly the length of its perimeter is 3 unit:

).



Now on the middle third of each side erect an equilateral triangle of side 1/3 unit; remove the base of each of these triangles so arriving at Figure 2

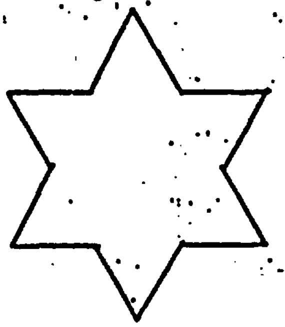
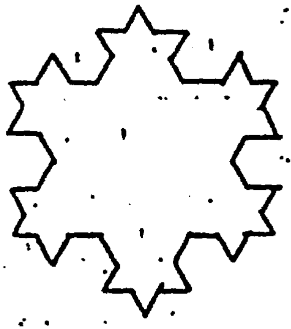


Figure 2 has 12 sides, each of length 1/3 unit; the length of its perimeter is therefore 4 units.

On the middle third of each of these 12 sides onstruct an equilateral triangle of side $^1/_9$ unit, then remove heir bases, so arriving at Figure 3 :



gure 3 has 48 sides each of length $^1/_9$ unit; the length of s perimeter is therefore $^{48}/_9$ units.

Continue in this way for n stages; it is easy see that after the n-th stage we will have a figure of $3(4^{n-1})$ es each of length $(\frac{1}{3})^{n-1}$ units giving a total perimeter of

$$3\left(\frac{4}{3}\right)^{n-1} \text{ units}$$

As

th

di

d

(N

ap

cu

din

is

req

tend

to t

(the

two

As n -> oo the length of the perimeter also -> oo although the figures are all contained in a finite area. The mathematical dimension of such a curve is defined to be the (unique) number d such that as n -> ∞

(Number of sides in the figure)x(length of each side)^{d} approaches a non-zero, finite value.

The existence of the unique number d for more general curves and surfaces and the consistency of this definition of dimension with the conventional one is due to Hausdorff and is dealt with in books on Measure Theory.

In the particular case of the figure above this requires the value of d to be that for which

$$\frac{3(4^{n-1})}{(3^{n-1})^{d}} = 3\left(\frac{4}{3^{d}}\right)^{n-1}$$

tends to a positive constant as n -> oo. Clearly we need to take d so that $3^{d}=4$ or:

$$d = \frac{\log 4}{\log 3} = 1.262...$$

(the base of the logarithms is immaterial, since the ratio of two logarithms is involved).

2. Quadratic iteration and the Mandelbrot set

A standard mathematical method for solving an equation $f(z)=0$ is to re-write it in the form

$$Z = F(Z) \qquad (2.1)$$

(which can be done in an infinity of ways) and then turn it into an iterative process by replacing Z by Z_n on the right of (2.1) and by Z_{n+1} on the left, viz:

$$Z_{n+1} = F(Z_n) \qquad (2.2)$$

We start from some arbitrary value Zo, use (2.2) to calculate Z_1, then again to calculate Z_2 and so on, and we hope that the sequence $\{Z_n\}$ converges to some value $Z=\alpha$ which satisfies (2.1) and hence our original equation i.e. $f(Z) = 0$. Unfortunately the process doesn't always converge though it will if Z_0 is not too far from α and $|F'(\alpha)|<1$, ("not too far" is very vague, but this needn't concern us here).

The simplest non-linear equation that we can be asked to solve is the quadratic

$$az^2 + bz + c = 0 \qquad (2.3)$$

By re-arranging terms and changing the variable if necessary one possible iterative method for solving such an equation may be written

$$Z_{n+1} = Z_n^2 + C \qquad (2.4)$$

We shall assume that C is, in general, a <u>complex</u> number If we start from $Z_0=0$, (2.4) gives $Z_1 = C$, $Z_2 = C^2+C$ and so on. There are 3 possibilities:

(1) the sequence $\{Z_n\}$ converges to a limit, α, which provides a solution of (2.4), and hence of (2.3),

(2) the sequence $\{Z_n\}$ does not converge but the points

:e

:s

:unately

not

but

(Z_n) remain within a bounded region of the complex plane for all n;

(3) the points (Z_n) eventually move outside any bounded region of the complex plane.

Consider a few cases:

(i) $C = -1;\ Z_0 = 0,\ Z_1 = -1,\ Z_2 = 0,\ Z_3 = -1$ ......
the sequence does not converge, but cycles with period 2; this is an example of case (2);

(ii) $C = 1;\ Z_0 = 0,\ Z_1 = 1,\ Z_2 = 2,\ Z_3 = 5,\ Z_4 = 26$,.....
the sequence $|Z_n|$ is clearly unbounded; case (3)

(iii) $C = i;\ Z_0 = 0,\ Z_1 = i,\ Z_2 = -1+i,\ Z_3 = -i,\ Z_4 = -1+i$,
the sequence does not converge, nor does it return to its original value, but it settles into a cycle of period 2; another example of case (2);

(iv) $C = -0.5;\ Z_0 = 0,\ Z_1 = -0.5,\ Z_2 = -0.25,\ Z_3 = -0.4375$,...
the sequence converges to one of the roots of the equation ($\frac{1}{2}(1-\sqrt{3}) = -0.366$ ...); this is case (1).

squa

othe

is as

This

entir

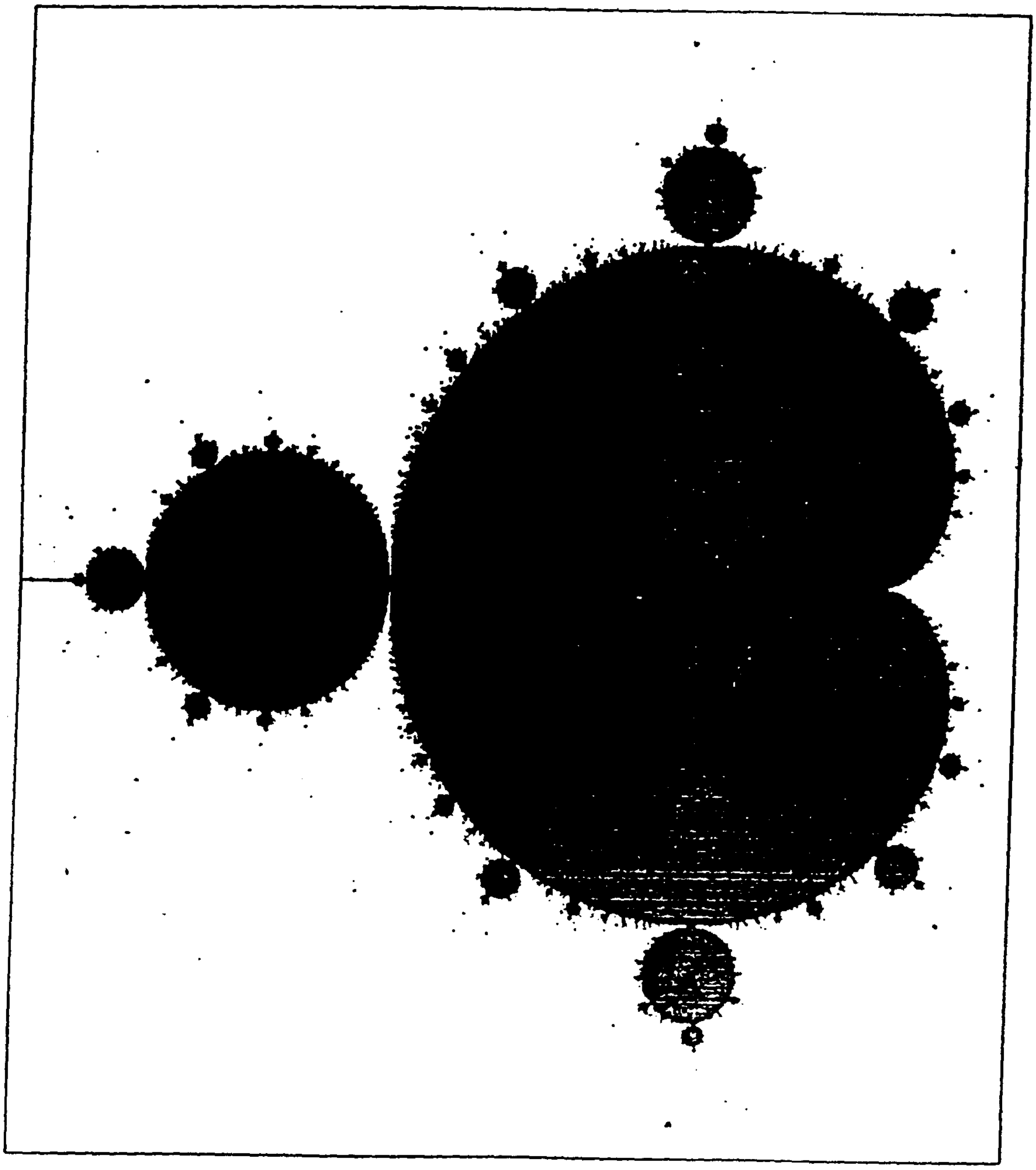
These examples show that each of the three possibilities (1), (2), (3) does occur for some values of the complex number C. Using a computer (even a micro will do) we can investigate for a lattice of values of C such as

$$C = (0.01)(j+ki), \quad -200 < j,k<200$$

starting (2.4) in each case with $Z_0 = 0.0$ and continuing for 100 iterations or until $|Z_n| > 2$ (which is sufficient to establish case (3)) to decide to which class ((1),(2), or (3)) each lattice point should be assigned.

If we adopt the convention that if a particular value of C leads to case (1) or (2) then the square of sides 0.01 with C at its centre is coloured black, otherwise it is coloured white we find that the black region is as shown.

This black region is called the Mandelbrot Set; it lies entirely inside the circle $x^2 + y^2 = 4$.



The Mandelbrot Set.

MANDELBROT AND JULIA SETS

The Mandelbrot Set, M, is defined by

$$Z_O = (0,0)$$

$$Z_{n+1} = Z_n^2 + c$$

$$M(c \text{ e } C, |Z_n| \nrightarrow \infty)$$

If P is any point on the boundary of the Mandelbrot Set we can study the set (of values of Z such that)

$$J_p(Z_O \varepsilon C, Z_n + 1 = Z_n^2 + P, |Z_n| \nrightarrow \infty)$$

which is the 'filled-in Julia Set' associated with P.

Using quite simple programs and a colour graphics screen remarkable pictures of Julia Sets can be generated.

Julia Sets are interesting from several points of view (mathematics, physics, control theory, turbul ent flow, biology...). They possess the 'Fractal property' (self-similarity) and are of fractional dimension.

For superb colour pictures of Julia sets see the books by Peitgen and Richter and by Peitgen and Saupe.

Black and white versions of some Julia sets (reproduced from my Presidential address to the IMA, (5)) are shown on the next slide. These were produced from output from the Cardiff Multics via Postscript on an Apple laser printer using an 800X800 mesh covering the square $- 2 < Re(z), Im(z) < 2$ giving a map about 7 inches square at a resolution of 115 pixels to the inch.

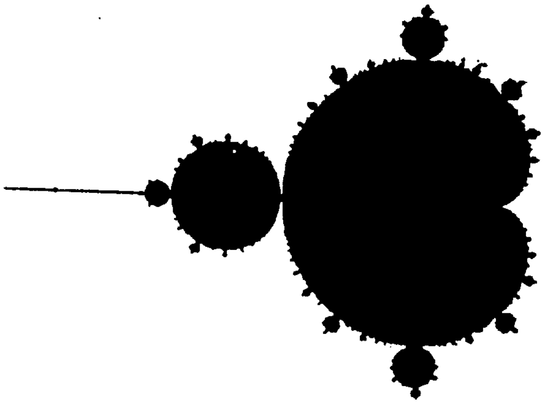


Fig. 4. Mandelbrot set

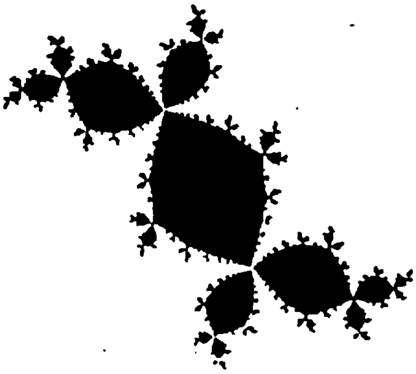


Fig. 7. Julia set attractive cycle of period 3 $(C = -0{\cdot}12 + 0{\cdot}74i)$

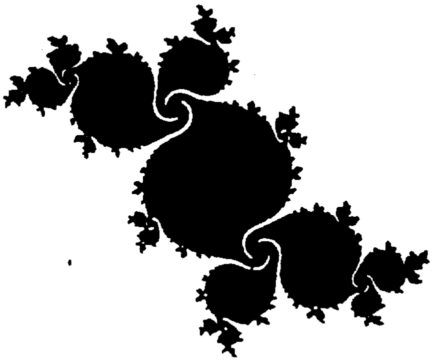


Fig. 5. Julia set associated with the point $-0{\cdot}11 + 0{\cdot}6557i$

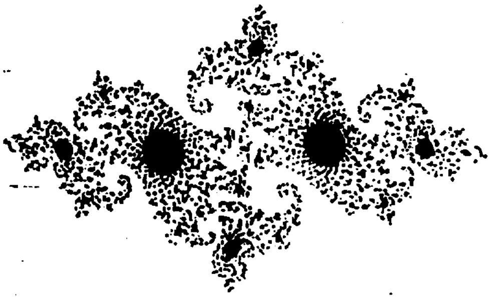


Fig. 8. Julia set of the region $-0{\cdot}745 + 0{\cdot}113i$

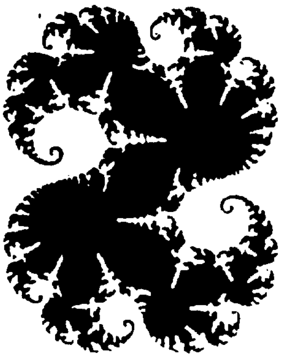


Fig. 6. Julia set associated with the point $0{\cdot}27334 + 0{\cdot}00742i$

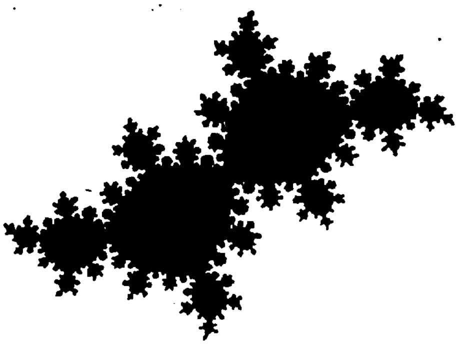


Fig. 9. Julia set associated with the point $-0{\cdot}39054 - 0{\cdot}58679i$

3. Affine Transformations

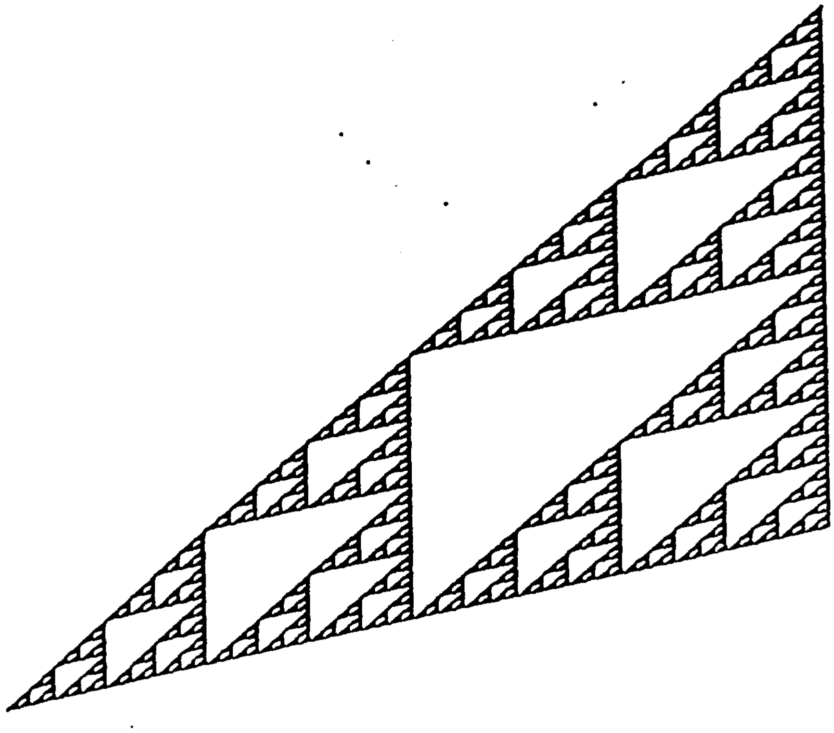
The Sierpinski Gasket

Let P_0, P_1 and P_2 be 3 arbitrary non-collinear points on a piece of paper. Let Z_0 be any point inside the triangle ABC. Let RAND(n) be a random number generator that generates 0, 1 and 2 with equal probabilities (i.e. $^1/_3$). A sequence of points Z_1, Z_2, ... is now constructed as follows:

$$\text{If RAND (n) = k then } Z_{n+1} = \frac{1}{2}(Z_n + P_k)$$

- that is, the new point Z_{n+1} is the mid-point of the line joining Z_n to whichever of P_0, P_1 or P_2 is indicated by the random number generator.

Generate a large number of points in this way and then reject the first few (10, say). If the points so generated are associated with the nearest points of a fine-mesh lattice and these "visited" lattice points are then coloured black with "unvisited" lattice points coloured white the resultant picture will be as shown below.



This .radordinary figure is often referred to as "the Sierpinski gasket" (or "Sierpinski triangle"). It can also be generated by an important general technique based upon affine transformations which may be defined in two dimensions as transformations of the (x,y) plane into itself by mappings of the type:

$$W\begin{pmatrix} x \\ \\ y \end{pmatrix} = \begin{matrix} a_{11}x + a_{12}y + b_1 \\ \\ a_{21}x + a_{22}y + b_2 \end{matrix}$$

For any such transformation there exists a constant S such that if $\underline{x}$ and $\underline{y}$ are any two points of R^2 and W(x), W(y) their images under W

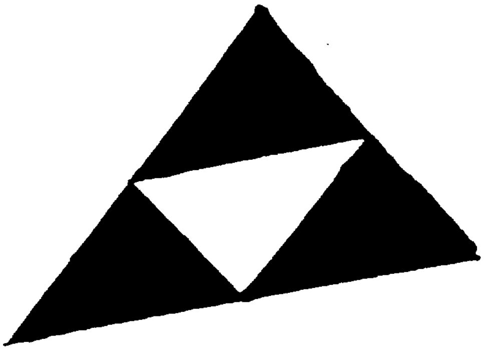
$$\|W(\underline{x}) - W(\underline{y})\| \le S\|\underline{x} - \underline{y}\|$$

The constant S is called the Lipschitz Constant of the mapping; if $S<1$ the mapping is said to be contractive: these are the transformations which are of most interest to us.

In the case of the Sierpinski gasket starting from the triangle $P_0P_1P_2$ we note that the gasket consists of three half-size copies of itself which are formed from the original triangle by the three affine transformations

$$W_i(Z) : Z \rightarrow \frac{1}{2}(Z+P_i) \quad i=0,1,2$$

One application of each of these three transformations to $P_0P_1P_2$ produces the figure



which has an area $^3/_4$ of the area of that of the original triangle.

Applying the three transformations to each of the sub-triangles and so on indefinitely produces the Sierpinski gasket. Since each iteration is applied to 3 fundamental regions of linear measure one-half of that of the previous fundamental regions the fractional dimension of the Sierpinski gasket is

$$\frac{\log 3}{\log 2} \doteq 1.585$$

(In general, a bounded region R which is the union of N non-overlapping sub-regions each of which is congruent to kR has fractal dimension logN/log $^1/k$.)

Iterated Function Schemes based on Affine Transformations

For the Sierpinski gasket we used three affine transformations, applying each of the three once at each iteration. We can generalise this process in a number of ways including:

(i) use more than three affine transformations;

(ii) apply the various transformations in a random manner with different probabilities;

(iii) the fundamental region from which we start need not be a triangle.

Combining all these generalisations a typical iterated function scheme (IFS) involves

(i) a region R

(ii) n affine transformations w_i with associated probabilities p_i (i=1,..,n).

Images of Clouds and Plants by IFS

If the transformations w_i are all contractive and the union of all of them applied to R

$$\bigcup_{i=1}^{n} w_i(R)$$

overlaps R itself to a considerable extent in that most, if not all, of R will be covered and some parts of R will be covered more than once, then an IFS provides a method for generating pictures of clouds, landscapes and plants. The method adopted is as follows:

(1) Choose a basic region, R, of approximately the desired shape;

(2) Cover R with a rectangular NxM mesh; associate a counter, initially set to zero, with each mesh point;

(3) Construct a set of contractive affine transformations $w_i(z)$ $(i=1,..,k)$ which collectively provide a covering of R to a considerable extent, with some overlap;

(4) Associate a set of probabilities $\{p_i\}$ with $\{w_i(z)\}$, $i = 1, .., k$,

(5) Let z_0 be a fixed point of one of the transformations i.e. $z_0 = w_i(z_0)$ for some i; let z_j be the most recent value of z obtained;

(6) Use a random number generator to choose an integer s, say, in the range <1,k>, where the probability of choosing s is p_s, and then apply w_s to z_j to produce a new value of z, $z_{j+1} = w_s(z_j)$.

(7) if (n_j, m_j) is the mesh point nearest to z_j increase the counter associated with (n_j, m_j) by 1;

(8) repeat steps (6) and (7) K times, say, where K is large compared to NxM;

(9) represent each of the NxM mesh points by a pixel and colour the pixel according to the counter associated with the mesh point.

By varying the probabilities $\{p_i\}$ the pictures displayed can be made to appear as if illuminated from various directions. For some very impressive examples of landscapes and plants generated in this way by Barnsley and others see [3].

The fractal dimension of such regions is not so easily found since some parts of R may not be covered at all and other parts may be covered more than once, and, in addition, the Lipschitz constants of the various transformations may be different. In the special case where R is exactly covered with no overlaps by the k affine transformations the fractional dimension is d where

$$\sum_{i=1}^{k} r_i^d = 1$$

and r_i is the scaling factor associated with the transformation $w_i(z)$.

4. Coastlines : Midpoint displacement

A method which has been used to generate fairly realistic looking coastlines is based upon a randomised version of the midpoint displacement method (which was used by Archimedes around 250BC to find the area enclosed by part of a parabola).

Let A and B be two points joined by a straight line and let d be the distance between them. Let C be the midpoint of AB.

$$A \underline{\quad d/2 \quad} C \underline{\quad d/2 \quad} B$$

We now displace C as follows: generate a Gaussian random number, g, with zero mean and unit variance and displace C a distance

$$gd2^{-h}$$

where h is a fixed real number in <0,1>. The intervals AC and CB are now bisected and their midpoints displaced by random multiples of

$$d2^{-2h}$$

..... and so on.

To approximate a coastline we begin with some fixed points on the coastline and join adjacent points by straight lines; midpoint displacements are then made in directions normal to the local straight line. A series of maps approximating to the map of Australia produced by Fournier et al [4] are shown below; the maps are based on 8 sample points and 8x127 points were interpolated with 4 different values of h (0.5, 0.7, 0.87, 1.0). The value of h is related to the fractal dimension, which for the coastline of Australia appears to be about 1.87, hence the choice in Map 12.

Instead of joining two adjacent data points by straight lines we could use cubic splines which would then provide higher orders of continuity - though these are only meaningful in a statistical sense.

A criticism of the midpoint-displacement method is that once a point has been positioned it is never moved again and a relatively large movement at an early stage in the process can be seen to persist throughout all the later stages which can produce a rather artificial effect.

of h
nsion,
e the

s we
rs of

nce a
large
ersist
tificial

Fig. 9. Australia: 8 Sample Points.

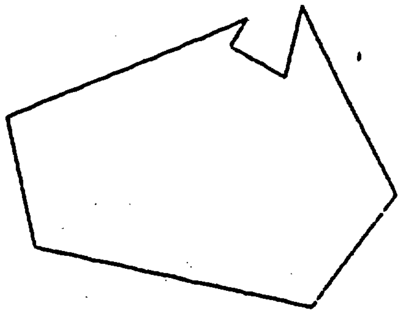


Fig. 10. Stochastic Interpolation. 8 original points and 8 × 127 interpolated points (h = 0.5).

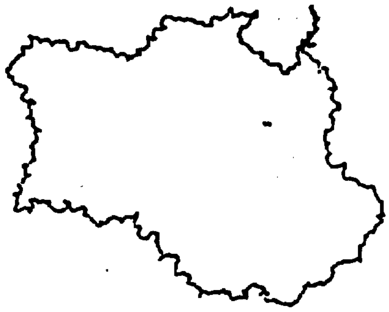


Fig. 11. Stochastic Interpolation. (h = 0.7).

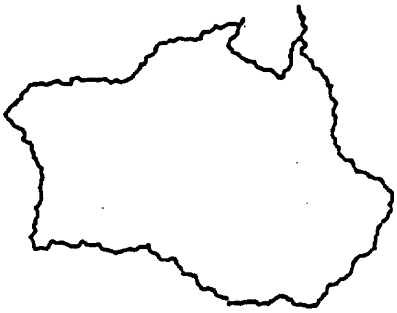


Fig. 12. Stochastic Interpolation. (h = 0.87).

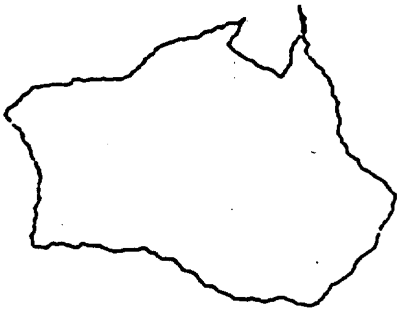
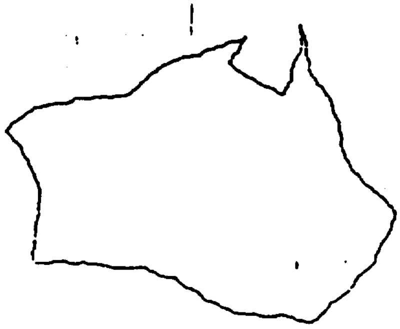


Fig. 13. Stochastic Interpolation (h = 1.0).



5. Fractals curves and string re-writing systems

It is possible to write instructions for a simple graph-drawing automaton ("a turtle") to produce some of the more angular fractal curves. The simplest such curve is the von Koch snowflake curve which can be generated by the following:

Algorithm (von Koch generation).

Let an automaton obey the following instructions on seeing the appropriate symbol:

Symbol	Action
F	draw a straight line a unit distance forward
+	turn right through the designated angle
-	turn left through the designated angle

On any other symbol, preserve the present state.

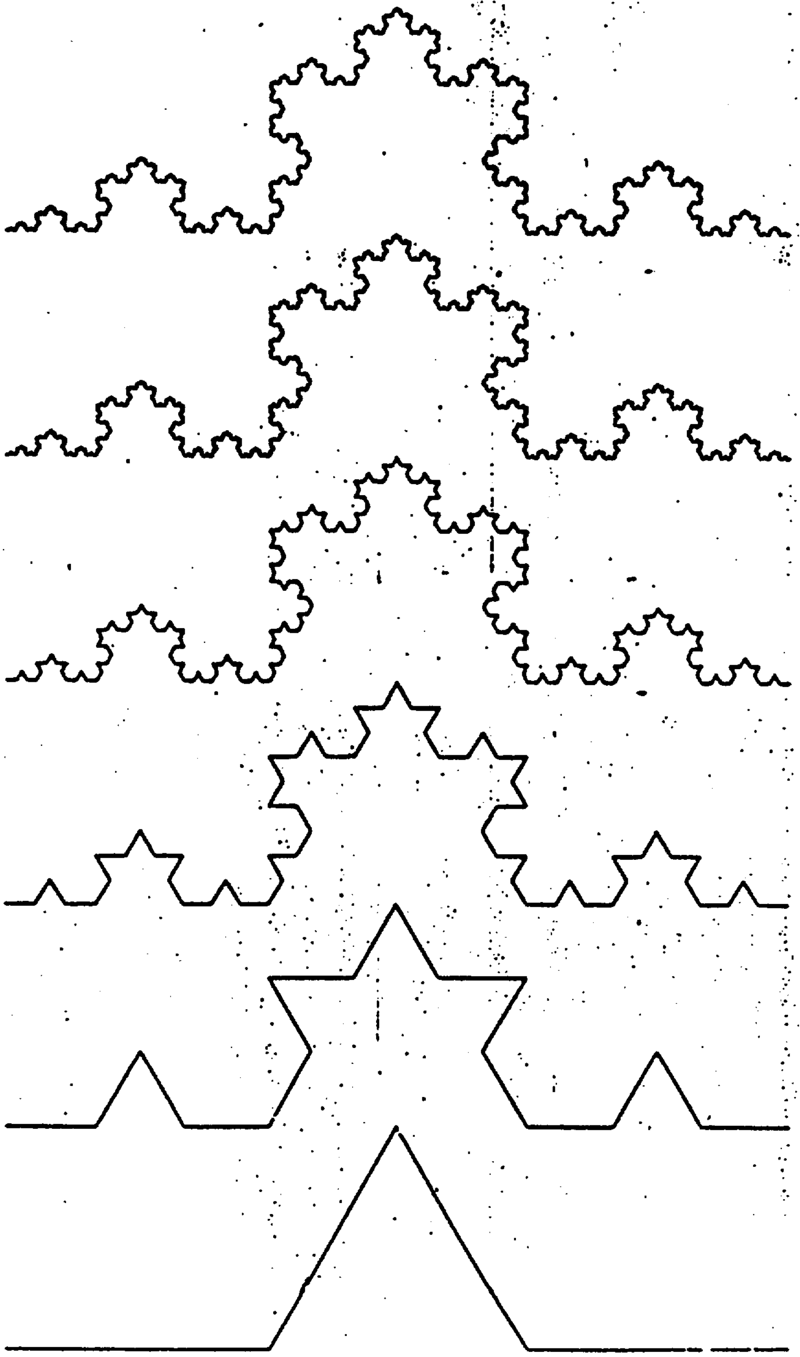
Then: (i) set the designated angle to 60° the cycle number = 0;

(ii) let the instruction be "F";

(iii) obey the instruction and increase the cycle number by 1;

(iv) replace F in the instruction by "F-F++F-F" and go to (iii) unless the cycle number exceeds N, in which case stop.

The first 6 stages in the generation of the von Koch curve are shown below:



For more complex curves the "production" rules are themselves slightly more complex, e.g. for the space-filling Peano curve, the first 6 stages of which are illustrated we have:

(i) let the cycle number be zero, the designated angle be $\pi/2$ and the instruction be X;

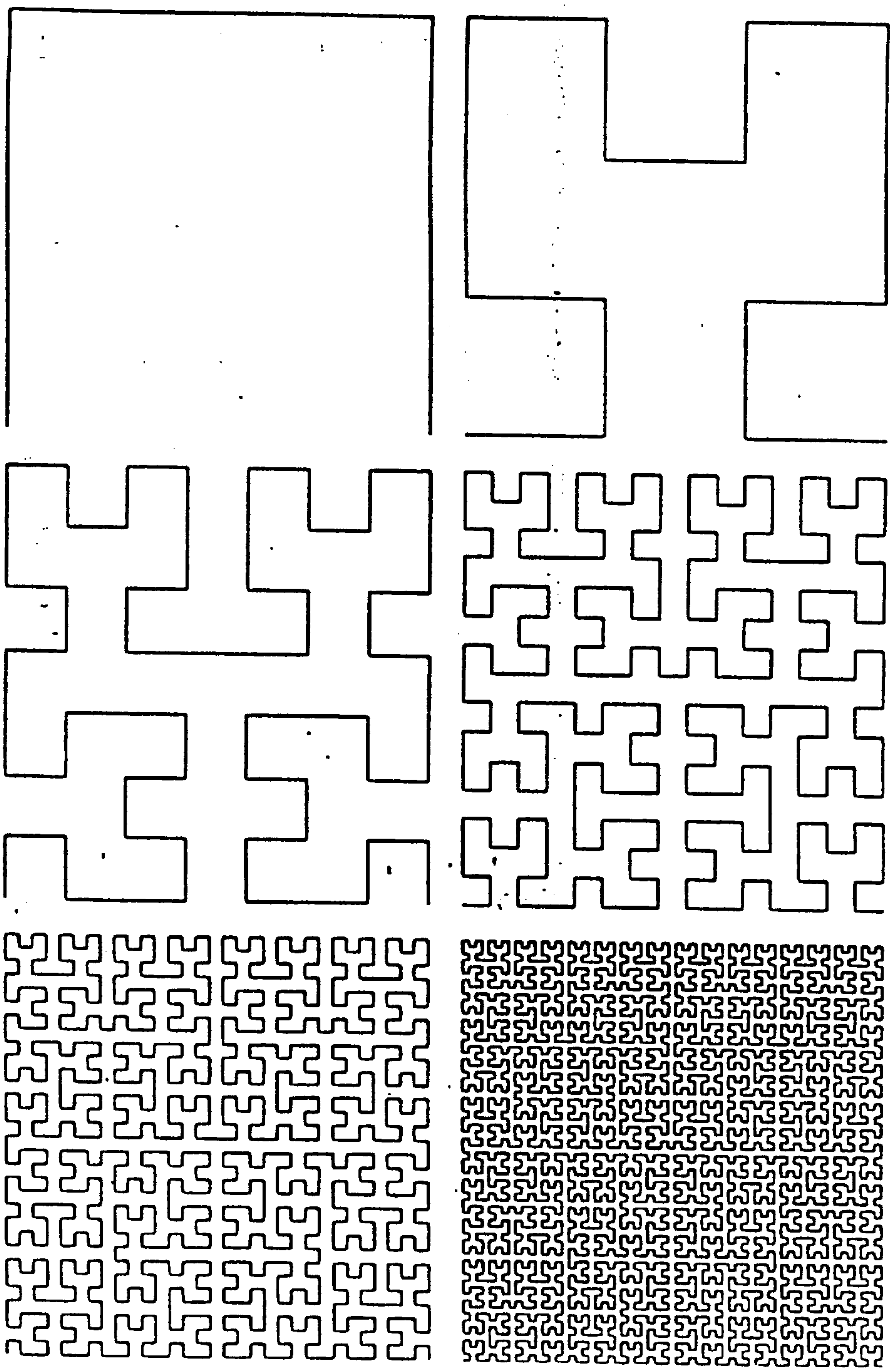
(ii) obey the instruction;

(iii) replace X by:- YF+XFX+FY-Y

and replace Y by : +XF-YFY-FX+

in the instruction; increase the cycle number by 1;

(iv) go back to (ii) unless the cycle number exceeds N.



6. LANDSCAPES ; USE OF FOURIER SERIES.

REALISTIC LOOKING LANDSCAPES HAVE BEEN PRODUCED BY MEANS OF 2-DIMENSIONAL FOURIER SERIES. THE HEIGHT OF THE SURFACE ABOVE THE POINT (x,y) IS COMPUTED FROM AN EXPRESSION SUCH AS:

$$Z(x,y) = \sum_{k=0}^{N-1} \sum_{m=0}^{N-1} C_{k,m} e^{2\pi i(kx+my)}$$

for $x,y = 0, \frac{1}{N}, \frac{2}{N}, \ldots, \frac{N-1}{N}$

WHERE THE COEFFICIENTS $C_{k,m}$ ARE RANDOM VARIABLES WITH

$$E(|C_{k,m}|^2) \propto (k^2 + m^2)^{-H-1}$$

It is then necessary to produce a slide showing how the landscape would look to an observer at a foreground point with illumination coming from a specific direction - this requires a lot of computation.

CERN Academic Training Programme

MAY 22nd - 26th 1989

FRACTALS

REFERENCES

1. B.B.Mandelbrot: "The Fractal Geometry of Nature", W.H.Freeman & Co., New York (1982).

2. H-O Peitgen and P.H.Richter: "The Beauty of Fractals", Springer-Verlag, New York; (1986).

3. H-O Peitgen and Dietmar Saupe (Eds.) "The Science of Fractal Inmages", Springer-Verlag, New York (1988).

4. Fournier, A; Fussell, D and Carpener, L. "Computer Rendering of Stochastic Models", C.A.C.M 25 (1982), 371-384.

5. Churchhouse, R.F: "Mathematics and Computers", Bull.I.M.A. 25 (1989), 40-49.