05/10/2004
News

Code−breakers, doughnuts, and violins

The British Association for the Advancement of Science (the BA) is a nation−wide organisation dedicated to connecting science with people and promoting openness about science in society. It organises Science Week (11−20 March 2005) and an annual Festival of Science, which was hosted this year by the University of Exeter. Mathematics was well represented at this year's Festival, with a morning of fascinating and engaging lectures on the Clay Institute Millennium Problems, an exhibition of mathematical art, a tour through the quiet streets of Exeter for a walking presentation on the life and work of William Clifford, and the launch of the National Cipher Challenge.

Million Dollar Maths

Image freeimages.co.uk

At the beginning of this millennium the Clay Mathematics Institute of Cambridge, Massachusetts, named seven Prize Problems. These were selected by a panel to span the most important unsolved problems in mathematics, and to generate interest and publicity for modern maths. As an incentive, each was allocated a prize fund of $1 million (£563,000) on acceptance of a proven solution.

The format of the Clay Prizes mirrors that of a similar challenge, issued a hundred years earlier in a famous speech by David Hilbert. In August 1900, Hilbert addressed the International Congress of Mathematicians in Paris and outlined 23 major problems he envisioned would direct research over the coming century. Although one of these problems was solved in only two years, the majority still withstand the attacks of the world's mathematicians. One in particular, Hilbert's eighth problem, is still very much open and has been reformulated and presented as a Clay Millennium Problem. The "Riemann hypothesis" was explained at the BA Festival by Marcus du Sautoy, who also described how the world of mathematics is currently abuzz with excitement over claims from a Frenchmen that he has finally proved it.

The seven Clay Prize Problems are:

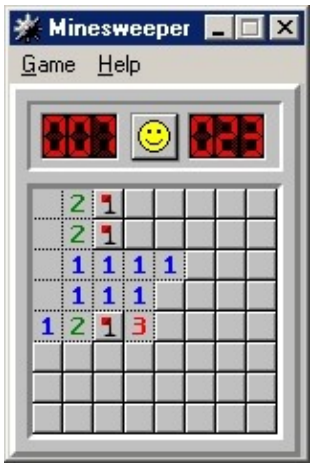
- P vs. NP;
- Riemann Hypothesis;
- Poincaré Conjecture;
- Birch and Swinnerton−Dyer Conjecture;
- Hodge Conjecture;
- Navier−Stokes Equations;
- Yang−Mills Theory,

more details of which can be found on the Clay Mathematics Institute website and in past issues of *Plus*. The first three problems on this list were spoken about at the BA Festival.

P vs. NP

Simon Singh is a well−known science broadcaster and the author of books including *Fermat's Last Theorem* and *The Code Book*. He began the morning of lectures by explaining the Clay Prize concerned with the difference between P−type and NP−type problems.

Some tasks are easy to accomplish. For example, imagine a line of cards with random numbers written on them that you must rearrange in ascending order. One method would be to look at each pair of neighbouring cards in turn, compare the two values, and swap their positions if the lower number is on the right. Repeat these three steps until no more swaps need to be performed on the entire line, and they will now be in ascending order. A simple step−by−step procedure like this for solving a problem is known as an algorithm. The algorithm here works relatively quickly − the length of time it takes to solve the problem (i.e. the total number of steps) increases only as a power of the size of the input (i.e. the number of cards). The algorithm run−time increases in polynomial time, and so the problem is called "P−type".



Playing minesweeper might be harder than you think.

Other tasks are much harder. The Travelling Salesman Problem involves finding the shortest path that passes through every one of a collection of points, like a salesman visiting a series of cities. Finding an optimal solution to this problem seems to be extraordinarily hard − the time taken by even the best algorithms increases much quicker than a power of the number of cities. In other words, as the problem gets bigger it soon becomes impossible to solve in a reasonable length of time. Such hard problems are said to be "non P−type". Finding the prime factors of an integer is also believed to be non−P, as is deciding whether any given position in the computer game Minesweeper is legal.

None of these have been proved to be non−P, however, because that would involve showing that no possible algorithm is capable of solving it in polynomial time. What has been achieved is to show that one class of problems, including the three just given, can be reformulated in each other's terms; i.e. if one can be solved in polynomial time then they all can. These problems are said to have "nondeterministic polynomial" running time − they are NP−type. One special property of NP−type problems is that although they are very hard to solve, the solution is simple to check. For example, it would take a while to find the two prime factors of 5,286,877, but a moment to check that 439 and 12,043 is in fact the right answer. An NP−complete problem is one whereby a shortcut polynomial time solution found to it implies that all other NP problems also have shortcut solutions.

The Clay Prize essentially asks for a proof that NP−type problems are in fact distinct from P−type ones; that no shortcut polynomial time algorithm exists to solve any one of them. If such a shortcut algorithm is found for a single NP−complete problem, then all of the NP−types are in fact P−type. Mathematicians expect all NP−complete problems to be non−P, but no one has been able to prove it yet.

Andrew Wiles making history

Singh also speculated as to the likely reaction to a Millennium Prize being awarded. In Fermat's Last Theorem he described what happened when Andrew Wiles solved this famous problem in 1994, after it had remained undemonstrated for over 350 years. The news was electrifying in mathematical circles, but also made the front page of newspapers around the world. Wiles himself become something of a celebrity figure, with appearances on TV programs such as Larry King Live on CNN, and even an offer from the clothing company GAP to model underwear!

The Riemann Hypothesis

Marcus du Sautoy is a professor of mathematics at the University of Oxford. His lecture was named after his book "Music of the Primes", and was essentially a live demonstration of the text. Prime numbers are integers with no divisors other than 1 and themselves. Because they cannot be decomposed any further du Sautoy calls them the atoms of arithmetic. As we saw above, no polynomial time algorithm is known for prime factorisation problem. It takes an impractically long period of time to calculate the two prime components of a large number, but not to multiply them to generate the number in the first place. This "one−way" function of multiplying primes is used to encrypt electronic information, such as your card number when you make a purchase online. du Sautoy illustrated this point about the modern importance of primes with a short clip from the Robert Redford film "Sneakers". Many mathematicians regard the Riemann Hypothesis as the most important unsolved problem in mathematics, he said.

Primes are also fascinating because they seem to be scattered randomly through the number line − it's impossible to predict where they might pop up. But it is much easier to estimate how many primes occur less than a particular number. For example, there are 4 primes less than 10, and 25 less than 100. Carl Friedrich Gauss discovered that you could make a fairly accurate guess at this frequency by treating the occurrence of a prime as the roll of a dice with a certain number of sides, which increases for higher numbers. There is a reasonably close match between a plot of this *logarithmic integral* function and the actual staircase of the primes.

Marcus du Sautoy

It was one of Gauss's students, G. F. B. Riemann, who saw how to achieve a better prediction, using a concept familiar to musicians (this was du Sautoy's cue to reach for his instruments). A tuning fork produces a single note − a pure sine wave. A violin playing the same note will sound distinct because it also generates harmonics of this fundamental note. This multitude of sine waves summates to produces a saw−tooth shaped vibration on the string. Summation of the harmonics produced by a clarinet, on the other hand, produces a square wave. Riemann's revelation was that the fundamental "note" of the function used by Gauss could be modified to the actual prime staircase by adding a set of specific "harmonics". Each of these harmonics corresponds to one solution of the "zeta function", which in fact has an infinite number of solutions. The astounding fact was that one of the components of all of the solutions that Riemann checked was 1/2.

The musical equivalent of this is that all of the harmonics are played with the same loudness − they are in perfect balance and none drowns out the others. Riemann had a gut instinct that all of the zeta function solutions fell on this critical line, but was unable to prove it. It has since shown to be true for the first 1.5 billion harmonics, but this does not imply that the infinity of them do. This, then, is the Riemann Hypothesis;

that every solution of the zeta function has a "real" part equal to 1/2. Proof of this hypothesis would win you the $1 million Clay Prize, and the fact that all harmonics play with the same loudness ensures that there really is no pattern to the distribution of the primes.

Professor Louis de Branges de Bourcia, a Frenchman now at Purdue University in the USA, claims to have done just that. But "the mathematical community is sceptical whether the methods of Louis de Branges are capable of proving the Riemann Hypothesis", du Sautoy explained. He continued to describe how the international community has underestimated de Branges before, however. "He became famous some years ago for proving one of Hilbert's great open problems, which initially was received with similar scepticism."

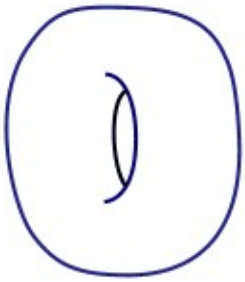
You can find more information about the music of the primes in an article by du Sautoy in issue 28 of *Plus*, or on the website for his book.

The Poincaré Conjecture

This third and final lecture on the Millennium Prize Problems was given by Keith Devlin, a consulting professor in the Stanford Mathematics Department, and former columnist for The Guardian newspaper. He presented the official Clay Mathematics Institute video on the problems, and has written the book *The Millennium Problems: The Seven Greatest Unsolved Maths Puzzles of Our Time*.

Keith Devlin

Henri Poincaré formulated his now famous conjecture on topology exactly 100 years ago. Topology (deriving from the Greek for the study of position) is the mathematical discipline concerned with surfaces or manifolds in higher dimensions. One example of a 2−dimensional manifold is the 2−sphere, like the surface of a football. Here the surface itself is 2−dimensional, but it is curved in the third dimension into a spherical object. The topology of surfaces is also called "rubber sheet geometry" because it studies what things are preserved during deformations. For example, the London Underground map is a distorted representation of the true geographical arrangement of stations, as if a map had been drawn on a sheet of rubber before it was stretched about. Only topological properties, such as the order of stations on the Bakerloo line, and which lines you can change to at Oxford Circus, are preserved. The geometric properties, such as true distance between stations, or the angles between lines, are not important.



A topologist doesn't even notice

The topology of two−dimensional planes curved into a closed surface (like a football) is more complicated. The classification of 2−dimensional manifolds was well established before Poincaré. It had been shown that if you take the sphere as basic, any other closed smooth surface can be obtained from it by manipulation. For example, tearing a hole in the middle of the sphere and rejoining the edges creates a "genus−1 torus", which will be more familiar to you as a doughnut. If another hole is torn into this surface it creates a "genus−2 torus", and so on. Under the rules of rubber sheet geometry any amount of stretching, twisting and moulding can be performed on the surface without fundamentally altering it. So in actual fact, a doughnut and a coffee cup are the same surface − they both have only one hole. (To be rigorous, the hole is not actually in the torus: the torus is the surface and the hole is in the space around the surface. An ant walking around the surface of a doughnut would never be aware of any edge or hole.)

So, it had already been proved for 2 dimensions that any manifold can be created by distorting a sphere, or the series of genus−n tori which are themselves generated from the basis. But what about 3−dimensional manifolds? This case is particularly important because the volume of our universe is believed to be a 3−dimensional surface that is curved in a fourth dimension.

Poincaré had assumed that he could use a method similar to that for 2D manifolds. He took the 3−sphere as basic and tried to show that any other smooth, closed 3−manifold could be obtained by manipulation. But he soon realised that even characterising what a 3−sphere is is not trivial, and this is crucial as the basis for understanding other 3−manifolds. A closed loop can be shrunk down to a point on 2−sphere, but not on a torus, demonstrating that they are fundamentally distinct manifolds. This is like wrapping a rubber band round a tennis ball and slowly rolling it off. This cannot be done round a doughnut, however, because the rubber band would reach the stage where it is constricted round the ring of the doughnut and cannot shrink any further. The Poincaré conjecture is that such an argument would work to define a 3D sphere (i.e. as the only 3−manifold without any holes), but he was never able to prove it to be true. The generalised Poincaré conjecture has since been shown for all dimensions greater than 4, but the original conjecture has so far remained unproven. Until now, that is.

A Russian mathematician, Dr. Grigori Perelman, submitted an abstract to an online journal in November 2002. In it he outlined his work on *Ricci flows* and the generalisation of 3−manifolds. If it is found to be watertight, Perelman will have proved a deep theorem known as Thurston's geometrisation conjecture. Poincaré's conjecture is a special case of Thurston's, and so if Perelman has in fact proved this Poincaré's will be immediately established as well. But Dr. Perelman has yet to submit a formal presentation of his proof, and appears to be unconcerned with the million dollar prize. In none of his papers or lectures has he even mentioned the Poincaré conjecture, and he refuses to talk to journalists about his work. The proof is likely to be nearly 100 pages long, and like Wiles's proof of Fermat's Last Theorem may take years to be rigorously checked by the only 30 or so mathematicians in the world qualified to do so. "Many experts think that Grigori Perelman's proof of the Poincaré Conjecture is correct but it is likely to take many more months before the experts are sure whether it is right or wrong", says Devlin.

The National Cipher Challenge

Simon Singh and Cipher Challenge organiser, Graham Niblo

After these three lectures Simon Singh launched the National Cipher Challenge 2004, organised by the University of Southampton. This is an internet−based competition for schoolchildren, consisting of a series of secret codes that must be cracked in order to win prizes. As author of *The Code Book*, a popular science book on the history of cryptography and code−breaking, Simon Singh was well−suited to introduce this exciting competition. He even brought along a genuine 1936 Enigma machine, used by the German Army to encode communications during the Second World War, and explained how it worked to generate encrypted messages that the Allies found nigh−on impossible to crack.

Lewis Dartnell

Plus is part of the family of activities in the Millennium Mathematics Project, which also includes the NRICH and MOTIVATE sites.