Great Moments in XXth Century Mathematics

In this issue we present the answers of two researchers, Gudlaugur Thorbergsson and Mark Pollicott, to the question "If you had to mention one or two great moments in XXth century mathematics which one(s) would you pick?".

Gudlaugur Thorbergsson

The most dramatic mathematical discoveries of the twentieth century might be the Gödel incompleteness theorem and the proof of Fermat's last theorem.

Instead of elaborating on these outstanding contributions, which are both far from the area that I have specialized in, I would prefer to reflect on what has impressed me from a more personal point of view, restricting myself to my own area of research.

We have witnessed enormous growth in Differential Geometry in the last quarter of a century. Gromov and Yau are clearly in the center of this development. Yau's solution of the Calabi conjecture is maybe the single most important result with important consequences in other areas like Algebraic Geometry. Gromov's most influential contribution might be his paper on pseudo-holomorphic curves which started a line of research in Symplectic Topology that recently culminated with a solution of the Arnold conjecture. One should also mention his highly original theory of hyperbolic groups and his numerous contributions to Riemannian Geometry.

If I look at the whole century and not only the few years that I have been able to witness personally, the theory of semi-simple Lie algebras and Lie groups and their representations comes to my mind. This is a theory that started in the last decades of the nineteenth century with the work of Killing and Cartan and took its final shape in the twentieth century with contributions of Cartan and Weyl and many others. First of all the beauty and intricate structure of this theory is fascinating. Then it is also central in so many areas of Mathematics that it certainly deserves to be considered as one of the the truly important contributions to Mathematics in the twentieth century.

Gudlaugur Thorbergsson was born in Melgraseyri, Iceland, having graduated from the University of Iceland. His postgraduate studies were done at the University of Bonn and he held positions at Bonn, IMPA - R. J. and University of Notre Dame. He is currently at the University of Köln. An important part of Professor Thorbergsson's research is in submanifold geometry. Recently he contributed a survey on isoparametric hypersurfaces and their generalizations to the *Handbook of differential geometry*, Vol. I, published by North-Holland.

Mark Pollicott

It is interesting that the XXth century began with a number of problems and conjectures which have helped to shape mathematical research and for 100 years (for example, the Hilbert problems and the Poincaré Conjecture) and concluded with the surprising solution of a far older conjecture (Wiles' proof of the Fermat Conjecture).

However, if I was asked to suggest some development of lasting importance and greatest impact then I might propose the work of Alan Turing on Mathematical Logic in the 1930s.

His conceptual development of what is now popularly known as a universal Turing machine anticipated the modern computer. His description of an abstract machine which can be made to carry out complicated tasks *through a combination of simple instructions inserted on a tape is easily recognised now as a description of a programmable computer (with the tape as the programme).*

Turing's motivation came from one of the most abstract of ideas in mathematics: The problem of "decidability" (Hilbert's second problem) which relates to whether, for a given well formulated mathematical problem, a solution necessarily exists or not. In the context of the Turing machine, given a finite set of instructions, it may be impossible to decide whether the machine would continue forever, or stop in some finite time.

The first practical application of Turing's ideas was during the second world war. Turing worked for the British Government Code and Cypher School on decoding military transmissions encoded by the german "Enigma" machines, developing practical decoding machines based on his original abstract ideas. The second important application of his ideas was the construction of the first programmable computer in Manchester under the aegis of Max Newman, in the late 1940s.

Mark Pollicott has held positions at the universities of Edinburgh and Warwick, as well as visiting positions at IHES, MSRI and IAS (Princeton). He was an Investigador Auxiliar of INIC from 1988-92, whereafter he took up a Royal Society University Fellowship at Warwick. He presently holds the Fielden Professorship in Pure Mathematics at Manchester University, England.

What's New in Mathematics

Race to settle Catalan conjecture: it's people vs. computers

Ivars Peterson reports in the December 2, 2000 Science on recent progress towards the resolution of this 150-year-old conjecture. Catalan noted that $8 = 2^3$ and $9 = 3^2$ are consecutive integers and conjectured that they were the only set of consecutive whole powers. This translates to the Fermat-like statement that the equation $xp - yq = 1$ has no whole-number solutions other than $3^2 - 2^3 = 1$. Recently Maurice Mignotte (Strasbourg) had given upper bounds on possible values of p and q; now Preda Mihailescu (ETH, Zürich) has shown that p and q must be a pair of "double Weiferich primes." Only six pairs are known, and, as Peterson reports, "a major collaborative computational effort has been mounted" to find more. You can help: volunteer at Ensor Computing's Catalan Conjecture page. Or you can join mathematicians who "are betting that a theoretical approach will beat out the computers."

Incompressible is incomprehensible

Why are some things so hard to understand? Jacob Feldman of the Rutgers Psychology Department has an answer, reported in the October 5, 2000 Nature. He found in a large set of experiments that for human learners, "the subjective difficulty of a concept is directly proportional to its Boolean complexity (the length of the shortest logically equivalent propositional formula)-that is, to its logical incompressibility." For example a concept which encodes as (A and B) or (A and not B) is equivalent to A and (B or not B), i.e. to A and so can be compressed to Boolean complexity 1. Whereas (A and B) or (not A and not B) cannot be compressed and has complexity 4. Subjects were asked to extract the concepts from sets of examples and non-examples. Main conclusion: "For each concept, learning is successful to the degree that the concept can be faithfully compressed." Feldman reflects on his result: "In a sense, this final conclusion may seem negative: human conceptual difficulty reflects intrinsic mathematical complexity after all, rather than some idiosyncratic and uniquely human bias. The positive corollary though is certainly more fundamental: subjective conceptual complexity can be numerically predicted and perhaps explained."

New encription algorithm

A new Federal encryption algorithm was reported in the October 20, 2000 Chronicle of Higher Education. The article, by Florence Olsen, relates how the Commerce Department, after a 4-year search, has declared the new federal standard for protecting sensitive information to