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

be Rijndael, an algorithm named after its inventors Vincent Rijmen and Joan Daemen. The two Belgians beat out 20 other entries, including teams from IBM and RSA. The new encryption algorithm, of which no mathematical details were given, can be made stronger as more powerful computer processors are developed. This was an entry requirement for the competition. According to Raymond G. Kammer of NIST, which managed the selection process, it should be good for about 30 years, "that is, if quantum computing doesn't manifest itself in five or six years."

Updating Ramanujan

The June 17, 2000 issue of Science News has a very complete and satisfying piece by Ivars Peterson about the recent discovery of new Ramanujan-type partition congruences. The n-th partition number p(n) is the number of different ways of expressing n as a sum of positive integers less than or equal to n. So $p(5) = 7$, as is easy to check, but these numbers grow very rapidly with n. Ramanujan discovered for example, that $p(5n + 4)$ is always a multiple of 5. (Thus $p(4) = 5$, $p(9) = 30$, $p(14) = 135$, $p(19) = 490, \ldots$). He also discovered similar congruences involving the primes 7 and 11. No one knew if those were all the possible partition congruences and if so, what was so special about 5, 7 and 11. Peterson recounts how Ken Ono, a number theorist at Penn State and Wisconsin-Madison, became interested in the problem and how he ended up proving that in fact there exist infinitely many partition congruences, work reported in the January 2000 Annals of Mathematics. Ono only gave one example: $p(an + b)$ is always a multiple of 13, where $a = 594 \times 13$ and $b = 111247$. (This gives an idea of why such congruences had not been found before!) His work was complemented in a remarkable way by Rhiannon L. Weaver, an undergraduate at Penn State, who developed an algorithm and used it to generate over 70000 new examples. Peterson quotes Ono: "It is now apparent that Ramanujan-type congruences are plentiful. However, it is typical that such congruences are monstrous."

Double Bubbles

In the March 17, 2000 Science is a piece by Barry Cipra: "Why Double Bubbles Form the Way They Do," and reporting on the recent solution of the Double Bubble Conjecture. The problem was to give a mathematical proof that the most economical way to enclose two contiguous given volumes is by a combination of three spherical surfaces, just as shown in John Sullivan's pictures. The solution, by Michael Hutchings of Stanford University, Frank Morgan of Williams College and Manuel Ritoré and Antonio Ros at the University of Granada, proceeds by showing that "any other, supposedly area-minimizing shape can be ever so slightly twisted into a shape with even less area."

Squeeze in a few more?

Kepler conjectured in 1611 that the most efficient way to pack equal-sized spheres (for example, identical oranges) in a box was to use the face-centered cubic configuration. It took a long time to settle this question to everyone's satisfaction. This finally happened two years ago, when Thomas Hales showed that the density of the face-centered cubic arrangement (approximately 74%) could not be improved upon. Then the question was considered, suppose the spheres are packed at random, like balls being poured into a container. Was there a maximum density for a random packing? Different experiments led to different estimates of this number, leaving a confusing situation. Charles Seife reports in the March 17, 2000 Science on the solution to this problem. There is no such number, and looking for it "makes no more sense than searching for the tallest short guy in the world." Random packings achieved with gentler and gentler pressure on the spheres can get arbitrarily close to Kepler's limit (and as they do so, they become more and more ordered). Seife is reporting on results recently published by S. Torquato, T. M. Truskett and P. G. Debenedetti, of the Complex Materials Theory Group at Princeton University, in the Physical Review Letters.

How to win $1,000,000 - the hard way

An Associated Press story, picked up by the March 26, 2000 Seattle Times, reports that Faber & Faber and Bloomsbury Publishing are offering a million bucks to whoever can prove that every even number is the sum of two primes. Simple? $2 = 1 + 1$, $4 = 3 + 1$, $6 = 3 + 3$, $8 = 3 + 5$, ...$98 = 79 + 19$, $100 = 97 + 3, \ldots$ but the problem has been open since its proposal in 1742. The stunt is in connection with the release of "Uncle Petros and Goldbach's Conjecture," by Apostolos Doxiadis. The million dollar assertion is in fact Goldbach's Conjecture. Good luck.

Originally published by the American Mathematical Society in What's New in Mathematics, a section of e-MATH, in

http://www.ams.org/index/new-in-math/home.html

Reprinted with permission.