THE
ABEL
PRIZE
2021

Proof beyond a reasonable doubt

To obtain a conviction in court, the prosecution is required to prove its case beyond a reasonable doubt. In mathematics this level of justification is in general not accepted as good enough. A mathematical proof should be deterministic, based on formal logic. The Pythagorean Theorem, stating that the sum of the squares of the two legs of a right-angled triangle equals the square of the hypotenuse, was already proved in the classical antiquity. The proofs (there are many of them) are deterministic since they can be reproduced and will provide the same result every time.

The development of high-speed electronic computers challenged the role of the deterministic proof tradition. It also paved the way for implementing algorithms which were far out of reach to do by hand. The new possibilities opened new questions. What are the limits of computation? How fast can we factorise an integer? Is it possible to verify something by using a probabilistic argument?

In general, it is a very hard task to factorise integers. If you choose a random 1000-digit integer and ask to find the prime decomposition, your computer may find the answer, but it is time-consuming. The sun might have burned out before you reach an answer. On the other hand, if you were given a candidate for the factorisation, it would in fact be an easy task for your computer to verify that the answer is correct. It is much harder to find a needle in the haystack, than verifying that it is in fact the needle you have found. This is the essence of a famous mathematical challenge, the so-called $\mathbf{P}$ versus $\mathbf{NP}$ problem, one of the seven millennium problems in mathematics.

The Abel Prize Laureates László Lovász and Avi Wigderson have been leading forces in the development of the mathematical foundations for theoretical computer science and its two complementary sub-disciplines: algorithm design and computational complexity. They have both made fundamental contributions to understanding the role of randomness in computation and to exploring the boundaries of efficient computation.

Lovász-Lenstra-Lenstra lattice reduction algorithm

An example of the laureate´s contributions within algorithm design is the so-called LLL lattice reduction algorithm, named after Lovász and the Lenstra brothers, Arjen and Hendrik. Given a higher dimensional integer lattice (grid), this algorithm finds a nice, nearly orthogonal basis for it. The algorithm has become a favourite tool for cryptanalysts, successfully breaking several proposed cryptosystems. It was also the basis for the disproving of the Mertens Conjecture.

The Mertens Conjecture was stated by Thomas Joannes Stieltjes in an 1885 letter to Charles Hermite and again in print by Franz Mertens in 1897. The conjecture is a statement about the Möbius function. The Möbius function, denoted μ, takes a natural number n as its input, and returns -1, 0 or 1 depending on the number of prime factors

of n; if n contains a square, the value is 0. The value $\mu(n)$ of a square-free number n is -1 if n has an odd number of prime factors and +1 if the number of prime factors is even. To state the Mertens conjecture you add all $\mu(n)$ for all positive integers less than some real number x and denote this sum by $M(x)$. The conjecture is that the square $M(x)^2$ is less than x for any choice of positive real number x.

The Mertens conjecture is a strong result. In fact, if the conjecture was true, it would imply the Riemann hypothesis, another one of the seven millennium problems in mathematics. Unfortunately this is a one-way implication, thus a disproof of the Mertens Conjecture has no consequences for the status of the Riemann hypothesis.

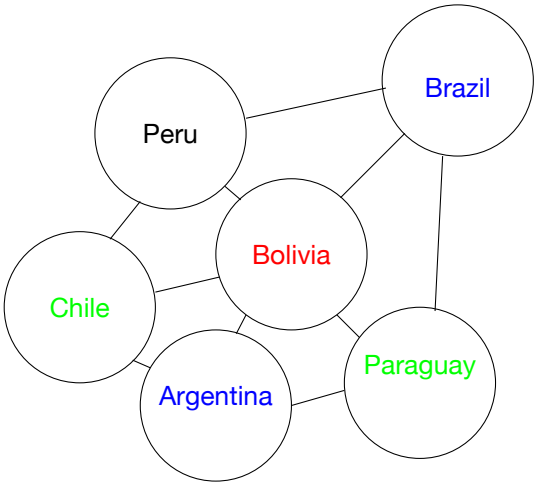
The Mertens Conjecture is a striking example of a mathematical conjecture proven false despite a large amount of computational evidence in its favour; after remaining unproved for almost a century the LLL lattice reduction algorithm made it possible for Andrew Odlyzko and Herman te Riele to finally disprove the conjecture.

Zero-knowledge proof

When you visit your bank to make a withdrawal, authentication is a crucial point. The bank must be sure that you are you, either you visit the bank in person or you enter the bank electronically. When you present the bank with your personal code, the bank must be able to verify that you are the true account owner. But, for security reasons, the bank does not want to store your personal code. So is it possible for the bank to verify a code it does not know? The answer is yes, using something called a zero-knowledge proof.

Zero-knowledge proofs were first conceived in 1985 by Shafi Goldwasser, Silvio Micali, and Charles Rackoff. Some years later Oded Goldreich, Silvio Micali, and Abel Prize Laureate Avi Wigderson developed the theory further, creating a zero-knowledge proof system for the graph colouring problem with three colours. This was extremely important, since the existence of this proof guarantees the existence of similar proofs for any problem of the same complexity.

The zero-knowledge proof system for the graph colouring problem with three colours goes as follows: Suppose we have given a separation of a plane into contiguous regions, as is the case of a map. Our task is to colour each country such that no adjacent countries have the same colour. In 1976 Kenneth Appel and Wolfgang Haken gave the first proof for the fact that, regardless of how the countries are located in relation to each other, it is possible to fulllfil the colouring task with only four colours. But suppose you only have three different colours. Then in general you will not be able to colour the map. Bolivia and its neighbouring countries is a nice example of this fact. Bolivia has 5 neighbours, Chile, Argentina, Paraguay, Brazil and Peru. The five neighbours surround Bolivia completely.



As we see in the illustration, where the connecting lines symbolise common borders, three colours is not enough.

On the contrary, suppose we have a map where it exists a colouring with only three colours. Is it possible for Alice to convince Bob that this is the case, without actually showing Bob the map? Wigderson et al. gave a positive answer; Alice covers the map so that Bob only sees the countries and the borders, but no colours. Bob picks two adjacent countries and asks Alice to uncover the colours. Alice obeys and Bob sees with his own eyes that the colours are different. Alice covers up the colours and Bob picks a new pair of neighbours for his colour check. Again Alice reveals the colours and Bob is satisfied with what he sees. So why does Bob not gain any knowledge from this procedure? The secret is that between two colour revelations Alice permutes the colours randomly. Thus what Bob experiences is that the two adjacent countries have different colour, - which colours is perishable information. After several steps Bob realises that the only possibility that Alice can succeed in every attempt, is that she actually has managed to colour the map with only three colours.

In this way Alice has provided Bob with a zero-knowledge proof. Zero-knowledge proofs are probabilistic, in the sense that the decisive argument for Bob is the overwhelming probability that Alice is right. He accepts Alice´s claim, as he finds it proven beyond a reasonable doubt.

Thanks to the leadership of the 2021 Abel Prize Laureates, theoretical computer science has found its place in modern mathematics. The probabilistic approach has proven to be a successful part of the mathematical universe, providing us with fruitful techniques and strategies. Beyond any reasonable doubt it has expanded our mathematical knowledge.