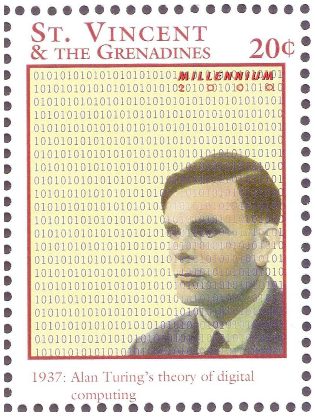
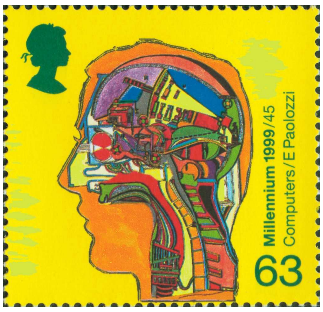
Alan Turing (June 23, 1912 – June 7, 1954)

by Heinz Klaus Strick, Germany

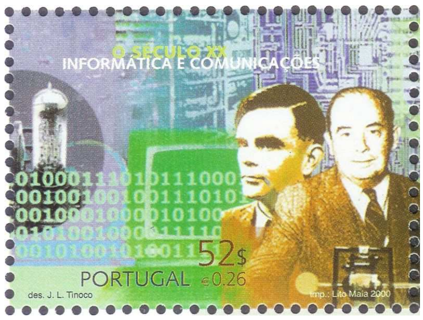


"So, on behalf of the British government, and all those who live freely thanks to Alan's work, I am very proud to say, we're sorry, you deserved so much better." With these words spoken in 2009, the British prime minister Gordon Brown expressed his regret for what had been done to the English mathematician Alan Mathison Turing fifty-five years earlier. The postal service of the Caribbean island St. Vincent honoured Turing in its millennium series of significant persons of the twentieth century, as did the Portuguese post, while Great Britain did no more than note the general progress that had been made in connection with the invention of the computer.

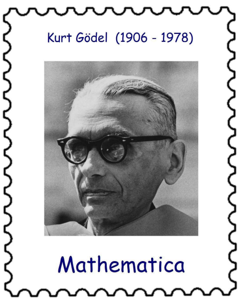


Alan Turing's father worked as an official in the British colonial service; his mother was born in India, where his father had been stationed as chief engineer for the Madras railway. Since the couple did not want their two children to grow up in the uncertain environment of the subcontinent, the mother returned to England to give birth to their son Alan. After a year, she returned to India, leaving the child along with his elder brother with friends. Alan saw his parents only on their occasional visits home.

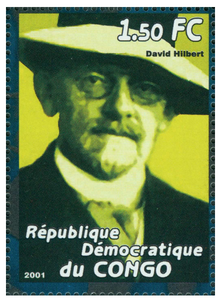
In his early school years, the boy did not make much of an impression. When at age 14, he was to transfer to a school one hundred kilometres distant, his start at that school was hindered by a nationwide transportation strike. However, in order not to miss even the first day of classes, the knowledge-hungry youth set off on his bicycle. Disappointed with the instruction at his new school, Alan Turing began to educate himself.



In his free time, Alan Turing immersed himself in Einstein's *theory of relativity* and Eddington's publications on *quantum mechanics*, while in his mathematics classes, he had to endure the criticisms of his teachers that he was not employing the prescribed methods in solving the assigned problems. Nonetheless, he won all the mathematics prizes that the school offered.



In 1931, he left for the University of Cambridge to study mathematics, and there he was finally able to pursue his own ideas. He was fascinated with John von Neumann's *Quantum Mechanics* and Bertrand Russell's *Introduction to Mathematical Philosophy*. He also took an interest in questions of mathematical logic. After passing his bachelor's examinations with distinction, he took an advanced course on the foundations of mathematics, where he encountered Gödel's discoveries about completeness and Hilbert's *decidability problem* (*Entscheidungsproblem*).



In 1900, Hilbert had posed the following question as one of the most important unsolved problems in mathematics: does there exist an algorithm by which for every (sufficiently formalized) mathematical expression it can be decided whether it is true or false? If there is such an algorithm that accomplishes this, then its existence can be most easily established by producing it. But how was one to prove that there can exist no such algorithm? And what should such a proof look like, which, after all, would itself be an algorithm?

In 1936, ALAN TURING, now a fellow at *King's College* in Cambridge, wrote the paper *On Computable Numbers with an Application to the Entscheidungsproblem*, in which he described a simple abstract calculational automaton that operates under a finite set of fixed rules. This automaton, today called a *TURING machine*, can perform only three operations: reading, writing, and moving its read-write head. On a theoretically infinite tape consisting of storage "cells" are written symbols (from a finite alphabet). Following a prescribed programme, a symbol is read or overwritten. Then the read-write head moves one cell to the left or right, or else halts. Numbers that can be computed by such a machine – the digits of such a number are written step by step on the originally blank tape – are called *computable*. For example, TURING showed that the number π is a computable number.

For every computable number one can specify an associated *TURING machine*. These TURING machines are *countable* in a natural way. Therefore, there can be only countably many computable numbers (and so due to the uncountability of the real numbers, most of them are *noncomputable*, or *undecidable*, in this sense).

Using the ideas behind CANTOR's diagonalization method, TURING described the properties that a noncomputable number has to possess, and he realized the paradox that consists in the fact that with a finite number of rules, he could describe a number that is not computable, although this finite number of rules itself defines a *TURING machine*. The problem is that there is no procedure by which one can decide whether a given *TURING machine*, no matter how defined, would complete the prescribed algorithm (*the halting problem*).

That these fundamental ideas were not immediately published is due the fact that ALONZO CHURCH, at Princeton University, had a few weeks previously submitted a paper with the title *An Unsolvable Problem in Elementary Number Theory*, and some of the ideas developed in that paper could also be found in TURING's work. TURING was compelled to add a reference to CHURCH in his article, in order to document the historically correct sequence of events, before his paper could finally be published. In the meantime, he accepted an invitation from CHURCH to continue his research at Princeton.

Returning to Cambridge, he hoped finally to realize an idea that had engaged him since his discovery of the idea of a *TURING machine*: the construction of a real computer. He was not thinking here of an electronic apparatus such as we know today, but an analog mechanical construction capable of processing a list of instructions. But nothing came of it. He was asked by the British government to help in breaking the German *Enigma code*.

When war broke out, the work of the team of scientists at *Bletchley Park* were subjected to the strictest secrecy. It was only in the 1970s that details of that work became known to the public.

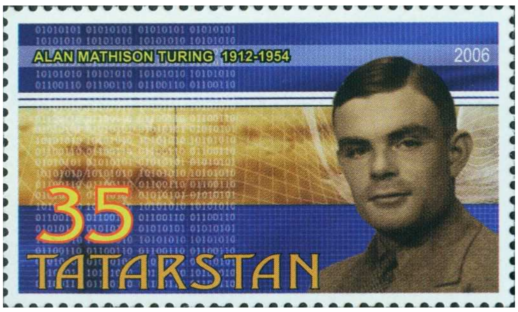
Around 1930, the German military services had begun to encode their communications with the help of *Enigma*, a machine with a number of gears connected in series, whereby the letters of the alphabet were permuted. However, the inventor of *Enigma* had succumbed to a fallacy in its construction: through the additional construction of a reverse rotor, the gears could be used twice for encryption, because the signals ran forwards and backwards through the gears; however, the number of possibilities was not thereby increased, but in fact decreased, since with such an arrangement, no symbol could be permuted to itself –the proportion of fixed-point permutations comes to about 37% (= 1/e).

The mathematicians MARIAN REJEWSKI, HENRYK ZYGALSKI, and JERZY RÓŻYCKI, recruited by the Polish secret service, managed in 1933 to build an electronic decoding machine that made it possible to run through all the possible gear positions of an *Enigma machine*. They named it *Bomba*, after a favourite type of ice cream. When the war began, they transferred their knowledge to the Allies. In the meantime, the *Enigma* had been further improved. The gears were replaceable, so that the time needed to decode a message increased. At the end of 1940, TURING supervised the construction of electromechanical machines that made it possible to decode the encrypted radio messages of the German Air Force and Navy in a very short time. (TURING "bomba"), not least thanks to the pivotal idea of subjecting the radio communications to statistical analysis. This was eventually automated by the construction of a first computer with over two thousand vacuum tubes (*Colossus*), to whose design TURING contributed greatly.

After the war, TURING was invited by the National Physical Laboratory in London to work on the development of a large mainframe computer (ACE = *Automatic Computing Engine*); in particular, he worked on the structuring of the programme for the computer. His forward-looking ideas regarding the necessary memory capacity of such machines were judged as excessive. For a time, he worked at the University of Manchester (Project MADAM = *Manchester Automatic Digital Machine*). His athletic ambitions led him to world-class times in middle- and long-distance races.

In 1950, the article *Computing Machinery and Intelligence* was published, in which TURING dealt with questions of artificial intelligence and developed what is today called the *TURING test*, through which one should be able to decide whether one is dealing with a human being or a machine.

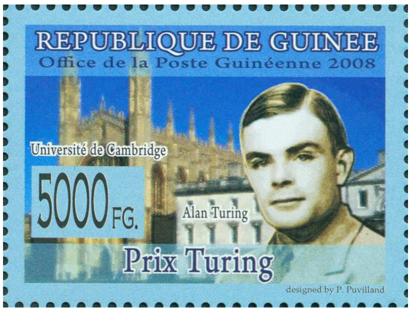
He was elected a member of the *Royal Society* in 1951. The focus of his research lay now in questions of theoretical biology, namely how patterns and forms arise in living beings. According to his ideas, pigments, such as the designs on animals' coats, arise from the fact that during embryonic development, chemical reactions take place at various diffusion velocities (*The Chemical Basis of Morphogenesis*, 1952).



The cold war between East and West meant that his research had to be kept secret. When someone tried to extort money from him by threatening to reveal his homosexuality, he went to the police, which led to his arrest and trial for the violation of laws against homosexual relationships. He was given the choice of going to prison or being subjected to oestrogen treatments.

His living situation deteriorated dramatically from then on. This ambitious athlete suffered physically from the oestrogen injections. Socially, his ostracism by those around him was noticeable, and not least, he was oppressed by being under constant surveillance by the security forces, in whose eyes he represented a security risk due to his involvement in secret projects.

He also suffered from the fact that his accomplishments could not be made known for reasons of secrecy, so that he felt a lack of general recognition. TURING died from cyanide poisoning, which a judicial investigation ruled a suicide.



In recognition of his contributions, the Association for Computing Machinery (ACM) has presented annually since 1966 the TURING Award, the highest honour for contributions to the field of computer science, comparable to the NOBEL Prize or the FIELDS medal.

First published 2011 by Spektrum der Wissenschaft Verlagsgesellschaft Heidelberg

https://www.spektrum.de/wissen/alan-turing-1912-1954/1072866

Translated by David Kramer

English version first published by the *European Mathematical Society* 2012