La vida y la obra de Alan Turing

Ricardo Peña Marí
Catedrático de Universidad de Lenguajes y Sistemas Informáticos

Departamento de Sistemas Informáticos y Computación
Universidad Complutense de Madrid

Seminario de Historia de la Matemática 2012/13, UCM 9 de enero de 2013

Outline

Infancia y juventud

- Su padre Julius trabajaba en el *Indian Civil Service* y estaba destinado en Madrás (India).
- Alan Mathison Turing nació el 23 de Junio de 1912 en Londres. Sus padres estuvieron el primer año con él y luego partieron de nuevo a la India, dejando a sus hijos al cuidado de un matrimonio amigo, los Ward.
- Tan solo se reencontraban en vacaciones, que pasaban en Irlanda o en Inglaterra.
- Pincelada sobre su personalidad a los 7 años: ¿donde tienen las abejas su colmena?

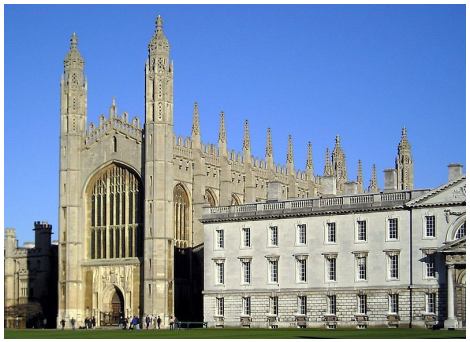
El instituto

Sherborne school

- Estudió en el Instituto Privado de Sherborne, una pequeña villa cerca de Southampton.
- Tenía curiosidad por muchas cuestiones (química, inventos), pero descuidaba las asignaturas que no le interesaban (la mayoría).
- Sacaba malas notas. A veces sus profesores se burlaban de él por su aspecto desaliñado, sus perennes manchas de tinta y su timidez.
- Otra pincelada: leía a Einstein a los 17 años, ¡y lo entendía!
- Tuvo un gran amigo, Christopher Morton, con el que compartía sus inquietudes científicas: astronomía, matemáticas, química.

Cambridge

- Después de Gotinga (Alemania), Cambridge era el centro de las matemáticas mundiales.
- Alan consiguió una beca e inició estudios de Grado en el King's College.
- Allí se interesó por los fundamentos de las Matemáticas y el "programa" de David Hilbert. Leyó a Gottlob Frege, Bertrand Russell, Kurt Gödel y John von Neumann.



Cambridge

- Tras el ascenso de Hitler al poder, en 1933 pasaron por Cambridge, camino de los Estados Unidos, Born, Courant, Shrödinger, y von Neumann, entre otros, y asistió a sus conferencias.
- En su trabajo de graduación (1934) demostró, sin conocer que ya lo estaba, el llamado Teorema Central del Límite, de importancia en Estadística.
- Su primera publicación en 1935 se inspiró en un trabajo de von Neumann sobre teoría de grupos. El propio von Neumann le animó a pedir una beca para una estancia en Princeton (EE.UU.).

El programa de Hilbert

En los Congresos de Matemáticas de 1900 y 1928 David Hilbert (Gotinga), propuso entre otros los siguientes problemas para ser resueltos en el nuevo siglo:

¿Es la aritmética consistente? ¿Se puede deducir de sus axiomas *cierto* = *falso*, o $1 = 0$?

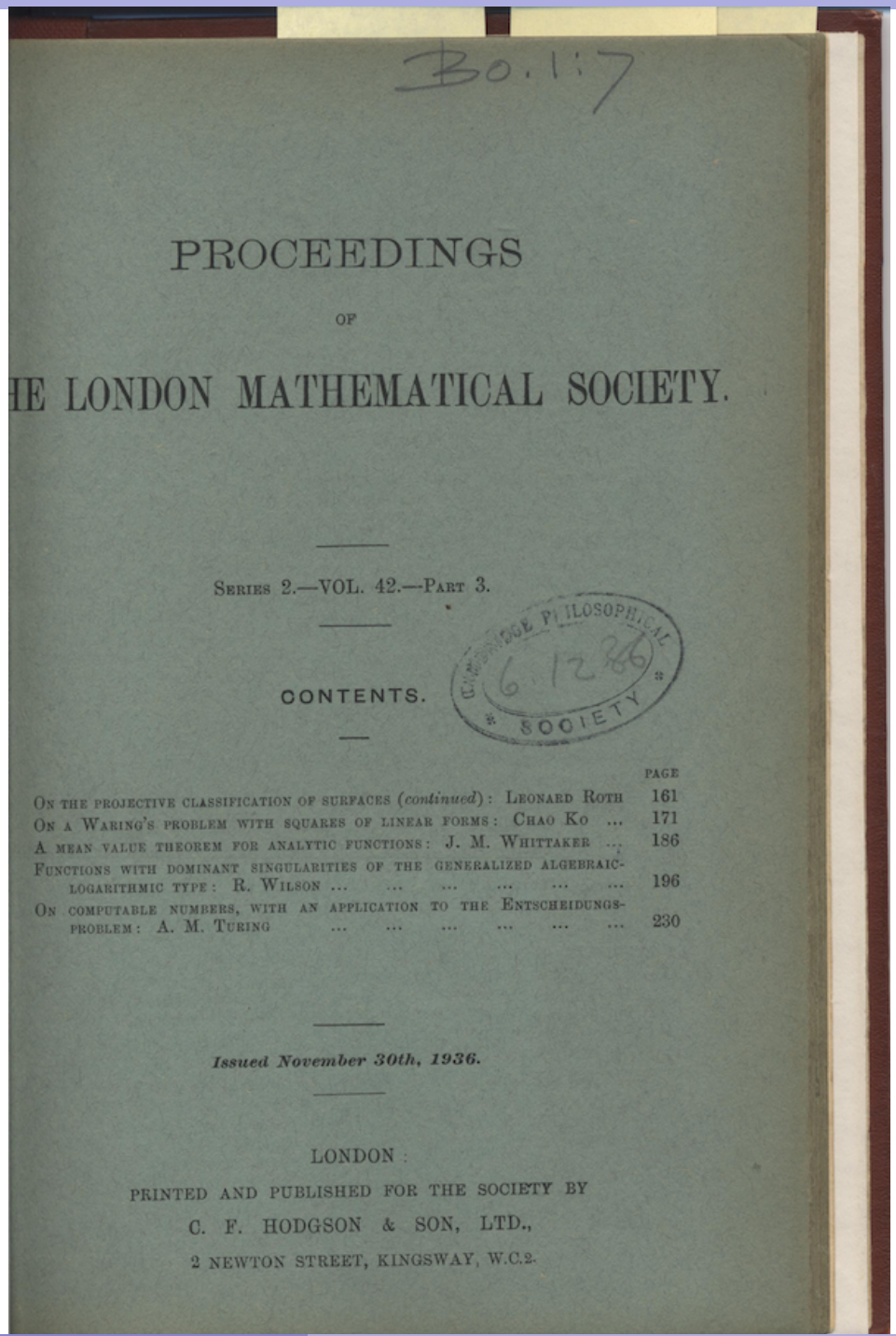
¿Es la aritmética completa? ¿Se puede deducir cualquier verdad de la teoría a partir de sus axiomas y reglas de deducción?

¿Es la aritmética decidible? ¿Se puede validar o refutar cualquier teorema mediante un "procedimiento efectivo"?

David Hilbert

El artículo de 1936

- El teorema de Gödel (1931) había dejado claro que si la aritmética era consistente, no era completa, es decir contenía verdades no deducibles.
- El artículo de Turing de 1936 contestó en negativo a la tercera pregunta: la aritmética contiene problemas que no son solubles mecánicamente.



Bo. 1:7

PROCEEDINGS

OF

HE LONDON MATHEMATICAL SOCIETY.

SERIES 2.—VOL. 42.—PART 3.

CAMBRIDGE PHILOSOPHICAL SOCIETY 6 DEC 1936

CONTENTS.

Issued November 30th, 1936.

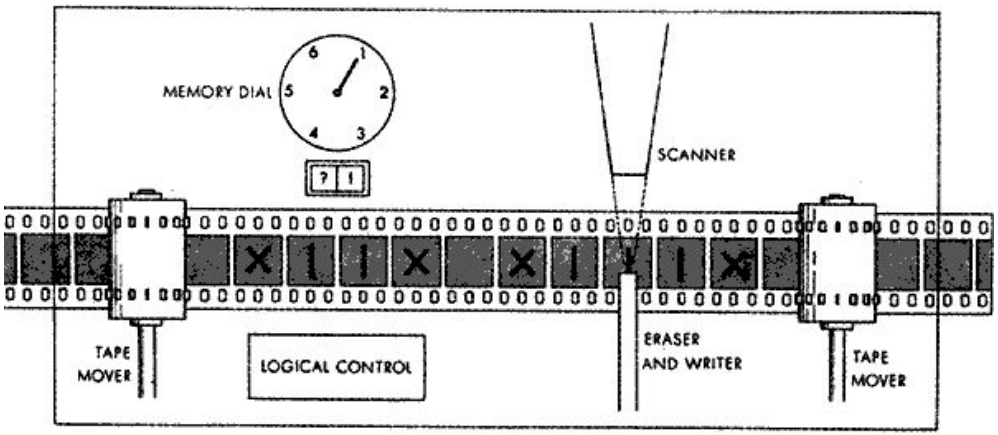
LONDON:

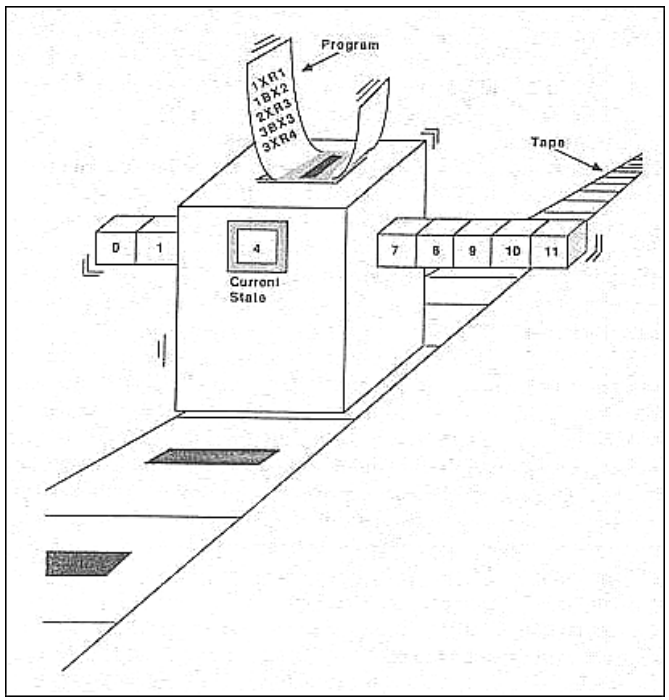
PRINTED AND PUBLISHED FOR THE SOCIETY BY

C. F. HODGSON & SON, LTD.,

2 NEWTON STREET, KINGSWAY, W.C.2.

La Máquina de Turing





- Su noción de "procedimiento efectivo"
- Símil con un calculador humano
- La cinta simboliza una fuente inagotable de papel
- La cabeza lectora/escritora, el punto de atención
- Los estados, las fases del cálculo
- La función de control, los pasos elementales del cómputo
- Insistencia en que el alfabeto de símbolos ha de ser finito
- El conjunto de estados, también
- La función de control puede modelizarse como un conjunto finito de tuplas (s_1, q_1, s_2, q_2, M), con $M \in \{L, R, N\}$.

¿Hay más números reales que Máquinas de Turing (MT)?

- Llamó números reales computables a aquellos para los que puede construirse una MT que calcule una tras otra todas sus cifras, si se le deja tiempo suficiente. Ejs: π, $\sqrt{2}$, $\log_3 5$, etc.
- Ideó un modo de codificar cada MT mediante un número natural único.
- Es decir, podía representar números reales de infinitas cifras mediante una descripción finita. ¿Podían representarse así todos los reales?.
- Era obvio que no había más MTs que números naturales.

El problema de parada

- George Cantor (1845-1918) ya había demostrado que había "muchos más" reales que naturales, es decir no se pueden poner en correspondencia biunívoca unos con otros.
- La conclusión obvia es que hay reales no computables. Eso ya indicaba que debía haber problemas no solubles por sus MT.
- De hecho encontró el más paradigmático, el problema de parada: No existe una MT que, dada la descripción de una MT cualquiera (mediante su número único) y una configuración inicial de la cinta para dicha MT, determine si la MT se parará o no ante dicha cinta.

La Máquina de Turing Universal

- Turing pensó que sus MT capturaban la noción de procedimiento efectivo, función computable, o simplemente algoritmo.
- Cada MT era una máquina especializada en un algoritmo concreto, determinado por su función de control.
- Pero Turing fue más allá e ideó una máquina universal que era capaz de emular a cualquier otra:
  1. Recibía en su cinta la descripción de la MT a emular, convenientemente codificada.
  2. Recibía en otra parte de la cinta (o en otra cinta, ya que probó que el número de cintas era indiferente para la potencia de las MTs), los datos tal como los esperaba la MT emulada.
  3. A partir de ahí se comportaba como lo haría la MT emulada ante esos datos.
- Si consideramos la descripción de la MT emulada como el "programa", había ideado una Máquina Universal programable, con el programa almacenado en memoria.

Princeton, New Jersey, 1936-38

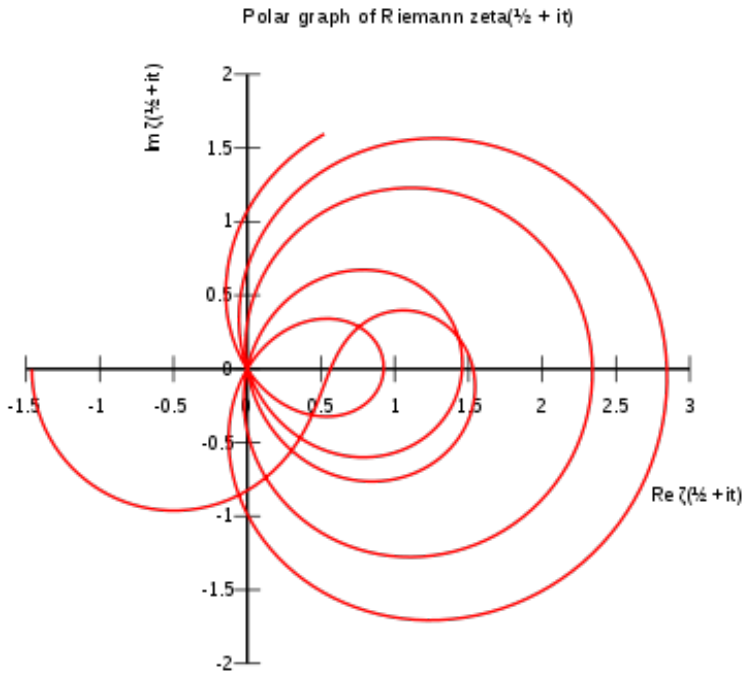
- En 1936 llegó a Cambridge un artículo de A. Church y S. Kleene resolviendo en negativo el problema de decisión de Hilbert, por un camino muy diferente al de Turing.
- Max H. Newman consideró no obstante que el trabajo de Turing merecía ser publicado. A la vez, escribió a Church pidiendo que permitiera a Turing trabajar con él.
- Alan marchó Princeton e hizo una tesis doctoral con Church. Trabajó con von Neumann, y conoció a otros científicos emigrados de Alemania.

Alonzo Church

Univ. de Princeton

La función-Z de Riemann

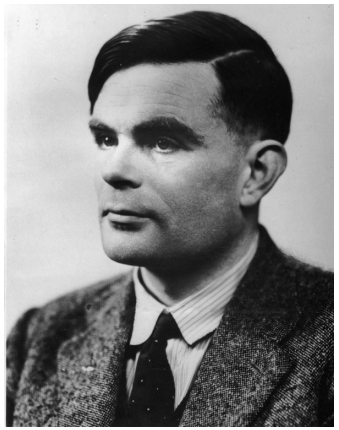
- Se interesó por la teoría de números. Planeó la construcción de una máquina para refutar la conjetura de la función-Z de Riemann (distribución de los primos).
- Ante lo inevitable de la guerra, redobló su interés por la criptografía: método de cifrado basado en multiplicar por grandes números y multiplicador binario con relés.
- Rechazó una oferta de von Neumann y regresó a Cambridge, donde le habían renovado su beca.



Función-Z

Bletchley Park

- La GCCS (*Government Code and Cipher School*), agencia del Servicio Secreto, estableció a 60 Km de Londres su centro de desciframiento de mensajes. En Bletchley Park llegaron a trabajar hasta 10.000 personas.
- En Agosto de 1939, Alan fue reclutado entre otros profesores, como experto en criptografía.
- El problema central era la máquina Enigma, usada por Alemania desde los años 20 y de la que existían versiones comerciales.
- Los matemáticos polacos llevaban 7 años de ventaja a los británicos y habían construido unas máquinas electromecánicas, las Bombas, para ayudar a descrifrar los mensajes de Enigma.

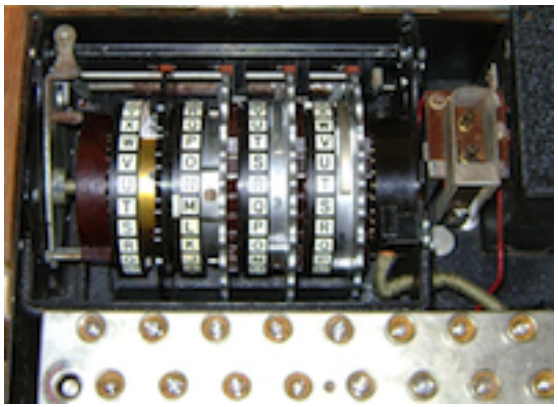


Bletchley Park

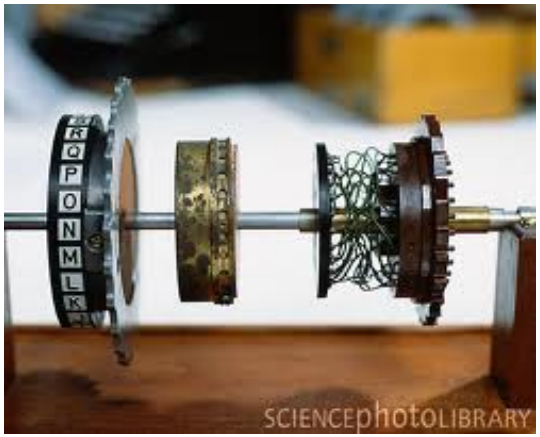
Enigma

Enigma

- El emisor tecleaba un mensaje como en una máquina de escribir. Enigma sustituía cada letra por otra.
- Cada rotor hacía una sustitución distinta según su cableado y tenía 26 posiciones iniciales, lo que daba $26 \times 26 \times 26 = 17.576$ configuraciones iniciales distintas.
- Al pulsar una tecla, el rotor más externo avanzaba una posición y generaba otra sustitución. Cada 26 avances de un rotor, se provocaba un avance del siguiente.



Rotores



Cableado rotores

Enigma

- Un panel de conexiones conectaba ciertas parejas de letras entre sí, lo que daba una sustitución adicional antes del primer rotor y otra después del último.
- Un anillo móvil de letras en cada rotor ($\times 17.576$).
- Los rotores eran intercambiables ($\times 6$ permutaciones).
- La codificación era simétrica: el receptor solo tenía que teclear el mensaje encriptado en una Enigma configurada igual que la Enigma emisora, y aparecía el texto original.

Teclado

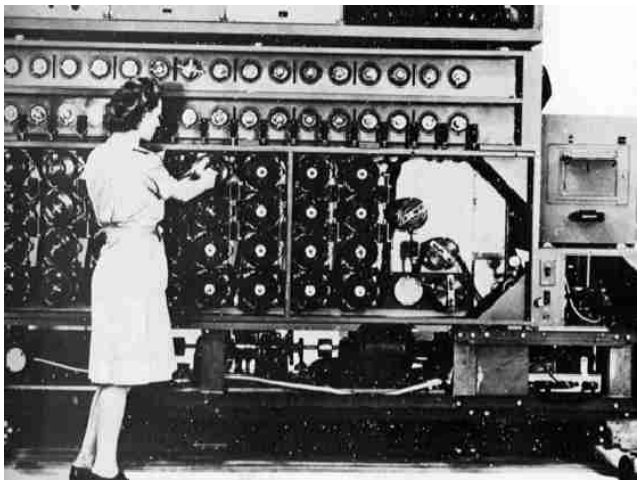
Panel

El uso de Enigma

- Órdenes diarias secretas para: (1) orden de los rotores; (2) posición de los anillos; (3) panel de conexiones; y (4) estado inicial de cada rotor.
- Antes de cada mensaje, el operador escogía al azar una nueva posición de los rotores, digamos XYZ, transmitía XYZXYZ en la configuración del día, colocaba los rotores en XYZ y transmitía el resto del mensaje.
- Los polacos usaron esa redundancia para descubrir la clave: coleccionando suficientes mensajes, y analizando las 6 primeras letras, establecían una "huella dactilar" única para la configuración del día. Tabularon las huellas en fichas perforadas.

El uso de Enigma

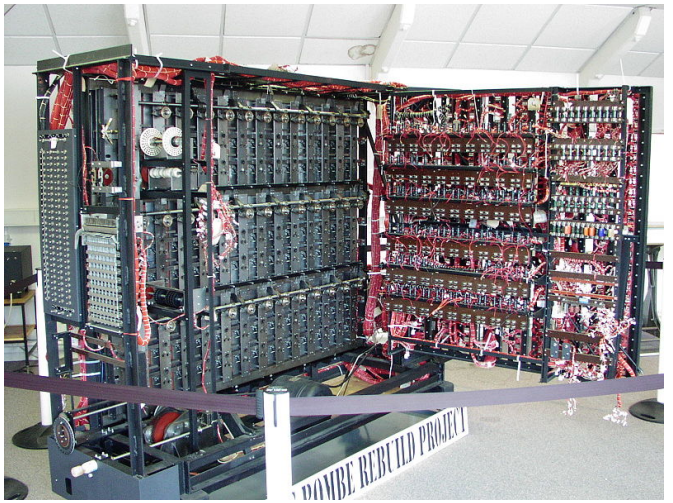
- El método era dependiente del uso de Enigma. Cuando cambió ese uso en Septiembre de 1938, sus fichas se volvieron inútiles.
- Con los nuevos indicadores de 9 letras encontraron otro tipo de huellas. Sus Bombas exploraban las 17.576 configuraciones de los rotores y se paraban al encontrar la huella buscada.
- Tenían 6 Bombas, una por cada permutación de los tres rotores. El método seguía dependiendo del uso. Además no trataban el panel de conexiones.



Bomba en operación

Las Bombas

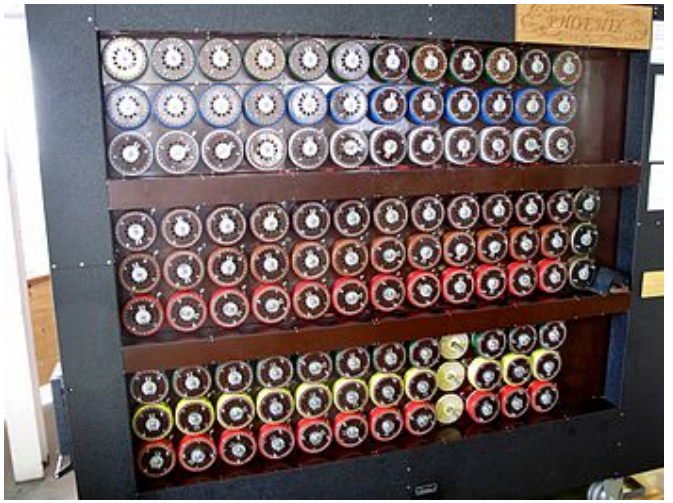
- En Diciembre de 1938, los alemanes aumentaron de 3 a 5 el juego de rotores. Ahora había 60 variaciones de 3 rotores, lo que implicaba 60 Bombas. Tambien aumentaron de 6 a 10 las conexiones del panel.
- La primera contribución de Turing fue generalizar las Bombas para que no dependieran de los indicadores ni del panel. La idea era suministrarle hipótesis en base al texto del mensaje y que ella descartara las combinaciones que entraban en conflicto con ellas.



Bombas reconstruidas en Bletchley Park

Las Bombas

- Las nuevas Bombas empezaron a construirse en 1940. Turing diseñó la mayoría de los circuitos.
- En 1940 pasó a dirigir "Hut-8", equipo responsable de la Enigma naval, que tenía un juego de 8 rotores, a elegir 3: 336 variaciones.
- Diseñó otras Bombas más generales que funcionaban por probabilidad. Desarrolló una teoría matemática específica.



Bombas reconstruidas en Bletchley Park

Nuevos retos

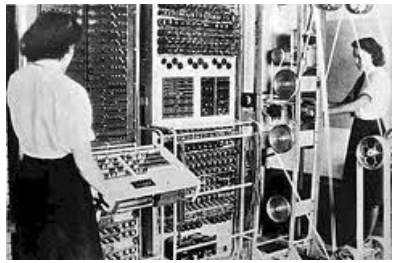
- Tras varias capturas de submarinos, comprendieron mejor la Enigma naval y consiguieron descifrar los mensajes en el día. Felicitados por Winston Churchill en 1941.
- "Apagón" en Febrero de 1942 al introducir los alemanes un cuarto rotor, esta vez fijo: $\times 26$. Los hundimientos en el Atlantico Norte alcanzaron cifras insostenibles.
- Se plantearon el uso de circuitos electrónicos para aumentar la velocidad.
- Nuevo código secreto Fish para los mensajes del alto mando alemán: máquina con 12 rotores, uso de cinta de papel y doble cifrado.

La era electrónica

- Errores alemanes les permitieron conocer la estructura de la máquina de Fish sin haber capturado ninguna.
- Max Newman (Cambridge) y Tommy Flowers (Postal Office) encargados de diseñar la máquina electrónica para descifrar Fish: Colossus.
- Turing contribuye con métodos estadísticos. Completada en 1943. Se construyeron 11 Colossus.
- A finales de 1942, Turing es enviado a EE.UU. por unos meses a entrenar a los analistas americanos en Enigma, a estudiar electrónica y a diseñar un método irrompible para cifrar voz.
- Se estima que las contribuciones de Alan Turing al desciframiento de mensajes, acortaron la Guerra en dos o tres años.

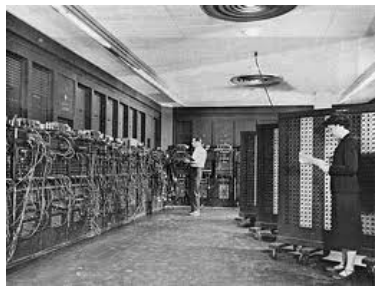
El National Physical Laboratory (NPL)

- El principal objetivo de Turing al acabar la guerra era construir un computador real con programa almacenado.
- En 1945 se completó en EE.UU. la ENIAC, (electrónica, J. Eckert, J. Mauchly, J. von Neumann) para calcular trayectorias balísticas. No era programable, aunque si más versátil que Colossus.
- El equipo de ENIAC comenzó a diseñar la EDVAC, cuya novedad sería almacenar el programa en memoria. En Junio de 1945, firmado por von Neumann, se publicó *Draft on a report on the EDVAC*.
- El report fue conocido por el NPL y el jefe de la División de Matemáticas (Londres) llamó a Turing para encargarle un proyecto similar.
- Turing aceptó el encargo y escribió un diseño muy detallado a finales de 1945. La máquina se llamaría ACE (*Automatic Computing Engine*).



Colossus 1943

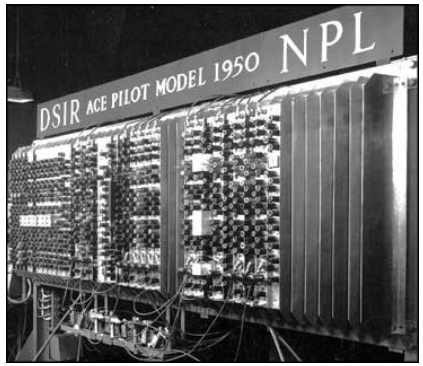
John von Neumann



ENIAC 1945

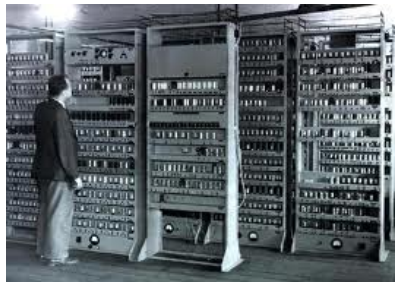
Los primeros computadores con programa almacenado

- Turing trabajó en la ACE hasta mediados de 1947. La mala gestión del NPL, las dificultades ingenieriles y la difícil comunicación con Turing, hicieron que este abandonara. Aún así, el proyecto se completó en 1950. Tenía una memoria de líneas de retardo de mercurio.
- Freddie Williams y Tom Kilburn, inicialmente subcontratados por el NPL, completaron un primer prototipo en la Universidad de Manchester. La memoria era un tubo de rayos catódicos almacenando 2.048 bits.
- Maurice Wilkes, de la Universidad de Cambridge, tras unos contactos iniciales con el NPL, emprendió su propio proyecto. La EDSAC fue el primer computador digno de tal nombre. Su memoria era de líneas de retardo.
- La EDVAC de von Neumann se completó en 1951, también con memoria de líneas de retardo.



ACE 1950


Manchester Baby 1948

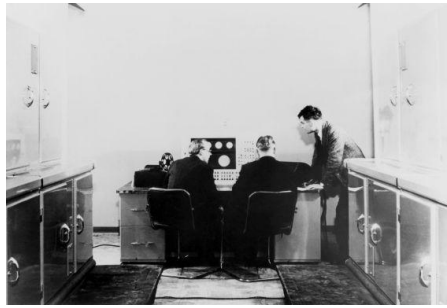

EDSAC 1949

Características de la ACE

- Desde el principio descartó una memoria de válvulas y se decantó, o por un tubo de rayos catódicos (a desarrollar por Williams), o por líneas de retardo.
- Decidió un diseño que minimizaba el hardware (caro) a costa de hacer más cosas por software, incluidas las operaciones aritméticas. En ese sentido se separaba de la línea dominante de EDVAC y EDSAC.
- Debía trabajar en binario. Escribió rutinas para transformar a/desde decimal.
- Énfasis en la rapidez. Reloj de 10^6 pulsos/seg.
- En lugar de incluir una instrucción de salto condicional, la simuló a base de automodificar el programa. Inspirándose en sus MT, trataba las instrucciones como números manipulables.
- Inventó el concepto de subrutina ("tablas" de instrucciones) que se llamaban entre sí jerárquicamente. Inventó dos instrucciones, `BURY` y `UNBURY`, que apilaban y desapilaban direcciones de retorno.

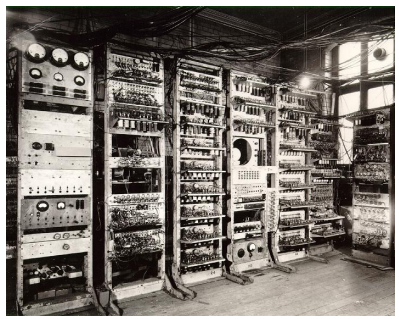
En la Universidad de Manchester

- En 1948, su profesor y amigo Max Newman le ofreció un puesto en la Universidad de Manchester para trabajar a las órdenes de Williams en el nuevo computador.
- Allí se dedicó sobre todo a programar rutinas, aunque tuvo alguna influencia en el sucesor del "Baby", la Ferranti Mark I, que tenía ya tres tubos de Williams y un tambor magnético para almacenar datos y programas.
- En esta época escribió *Checking a large routine*, primer precedente histórico del uso de la lógica de predicados para razonar sobre los programas.
- Con esta máquina demostró que los primeros 1.540 ceros de la función-Z de Riemann estaban en la recta crítica.



Turing ante la consola de la Mark I

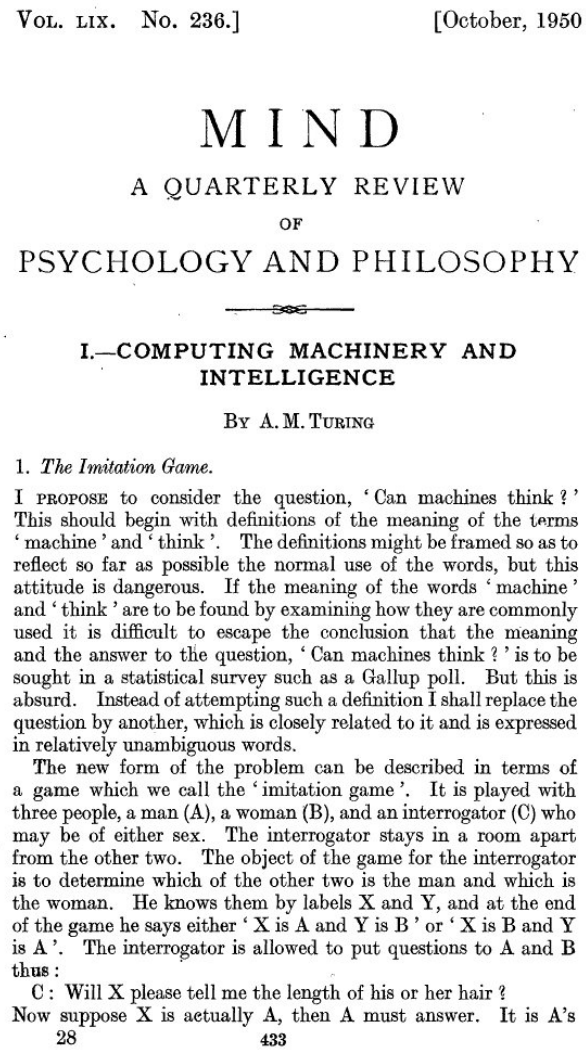
Freddie Williams



Mark I 1951

Los fundamentos de la Inteligencia Artificial

- Turing escribió dos artículos, que después han sido ampliamente citados: *Intelligent Machinery (1948)* y *Computing Machinery and Intelligence (1950)*.
- En el primero establece las bases del conexionismo y del aprendizaje artificial por medio del entrenamiento. Esta línea ha fructificado actualmente en lo que se conoce como redes neuronales.



VOL. LIX. No. 236.] [October, 1950

MIND

A QUARTERLY REVIEW

OF

PSYCHOLOGY AND PHILOSOPHY

I.—COMPUTING MACHINERY AND INTELLIGENCE

BY A. M. TURING

1. *The Imitation Game.*

I PROPOSE to consider the question, 'Can machines think?' This should begin with definitions of the meaning of the terms 'machine' and 'think'. The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous. If the meaning of the words 'machine' and 'think' are to be found by examining how they are commonly used it is difficult to escape the conclusion that the meaning and the answer to the question, 'Can machines think?' is to be sought in a statistical survey such as a Gallup poll. But this is absurd. Instead of attempting such a definition I shall replace the question by another, which is closely related to it and is expressed in relatively unambiguous words.

The new form of the problem can be described in terms of a game which we call the 'imitation game'. It is played with three people, a man (A), a woman (B), and an interrogator (C) who may be of either sex. The interrogator stays in a room apart from the other two. The object of the game for the interrogator is to determine which of the other two is the man and which is the woman. He knows them by labels X and Y, and at the end of the game he says either 'X is A and Y is B' or 'X is B and Y is A'. The interrogator is allowed to put questions to A and B thus:

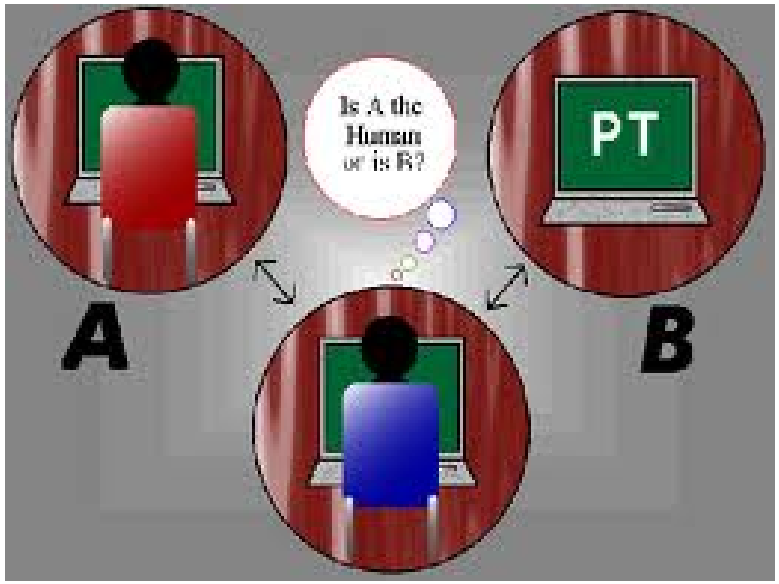
C: Will X please tell me the length of his or her hair?

Now suppose X is actually A, then A must answer. It is A's

28 433

The Imitation Game

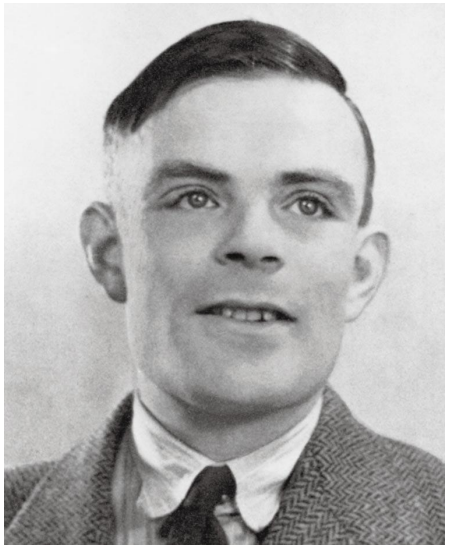
- El segundo es de carácter más filosófico y se plantea la pregunta de si es posible emular la inteligencia en una máquina.
- Aquí es donde propone el conocido Test de Turing en el que una máquina intenta confundir a un observador, que solo puede leer sus respuestas, haciéndole creer que es un humano.



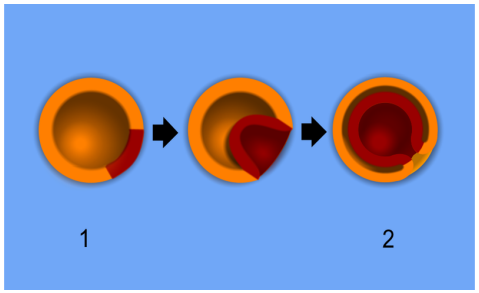
El Test de Turing

Modelos de morfogénesis

- Cumplido su sueño de contribuir a la creación y programación de máquinas reales, su atención se dirige hacia otra de sus inquietudes científicas: las matemáticas de la formación de patrones biológicos.
- ¿Cómo se elige una dirección privilegiada en la gastrulación? ¿Cómo se forman las manchas en la piel de algunos animales? ¿Por qué están presentes los números de Fibonacci en las piñas y en los girasoles?



A. M. Turing en 1948

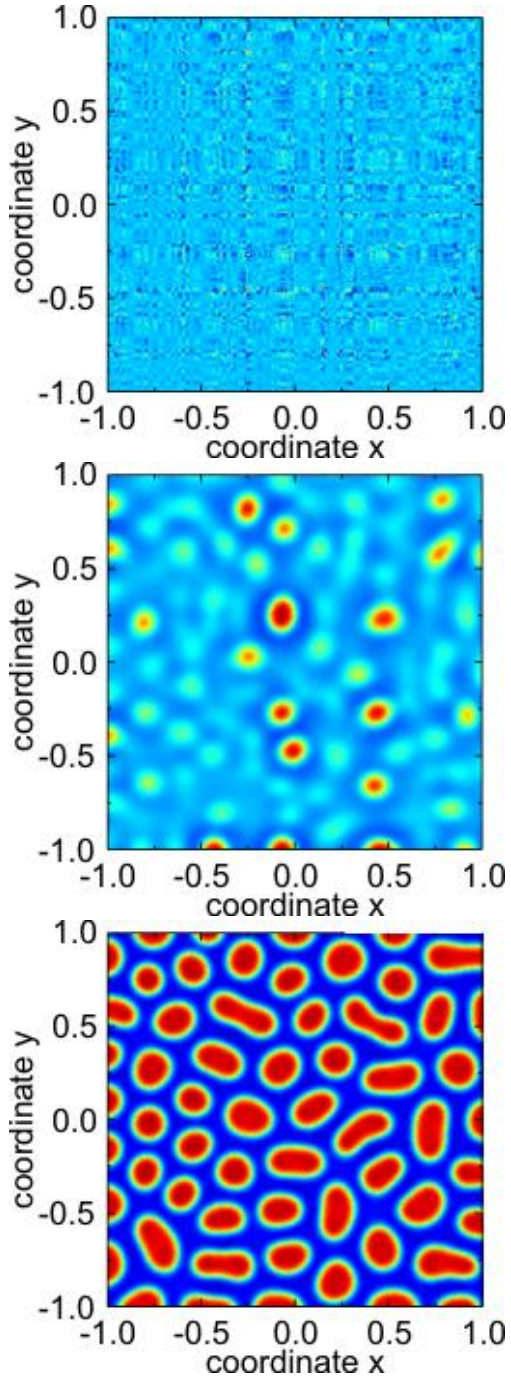


Gastrulación

Manchas

El modelo en acción

- Plantea un sistema de ecuaciones diferenciales que modelan la interacción de dos agentes químicos o morfogenes: un activador y un inhibidor.
- Su trabajo de 1952, *The Chemical Basis of Morphogenesis*, muestra convincentemente que esos patrones son solución de sus ecuaciones.
- Recientemente (*Nature Genetics, Feb. 2012*) se han identificado con precisión el mecanismo y los morfogenes predichos por Turing.



Persecución, crisis y muerte prematura

- Un amigo de un amante ocasional robó en su casa y Turing lo denunció a la policía. En el interrogatorio la policía se centró en su homosexualidad, que él no trató de ocultar.
- La combinación de haber "cometido" lo que en la Inglaterra de la época era un grave delito, ser poseedor de importantes secretos militares, y la atmósfera de guerra fría de esos años, hizo que fuera juzgado y condenado.
- Se le dio a elegir entre la cárcel y la castración química. Fue sometido a un fuerte tratamiento hormonal que le ocasionó varias crisis depresivas.
- Al mismo tiempo, sus visitas eran investigadas y la policía le tenía bajo una estricta vigilancia.
- Fue encontrado muerto en su cama el 8 de Junio de 1954, envenenado por una manzana a medio comer impregnada en cianuro. Según su madre, su muerte fue accidental, pero la mayoría de los historiadores y la propia policía diagnosticaron suicidio.

El legado de Turing

Los informáticos somos herederos de los campos que el abrió para la ciencia. Nos dejó muchos ejemplos: su generosidad, su desprendimiento de las cosas mundanas, y sobre todo, su pasión ilimitada por el conocimiento.

Estatua de Alan Turing en Bletchley Park