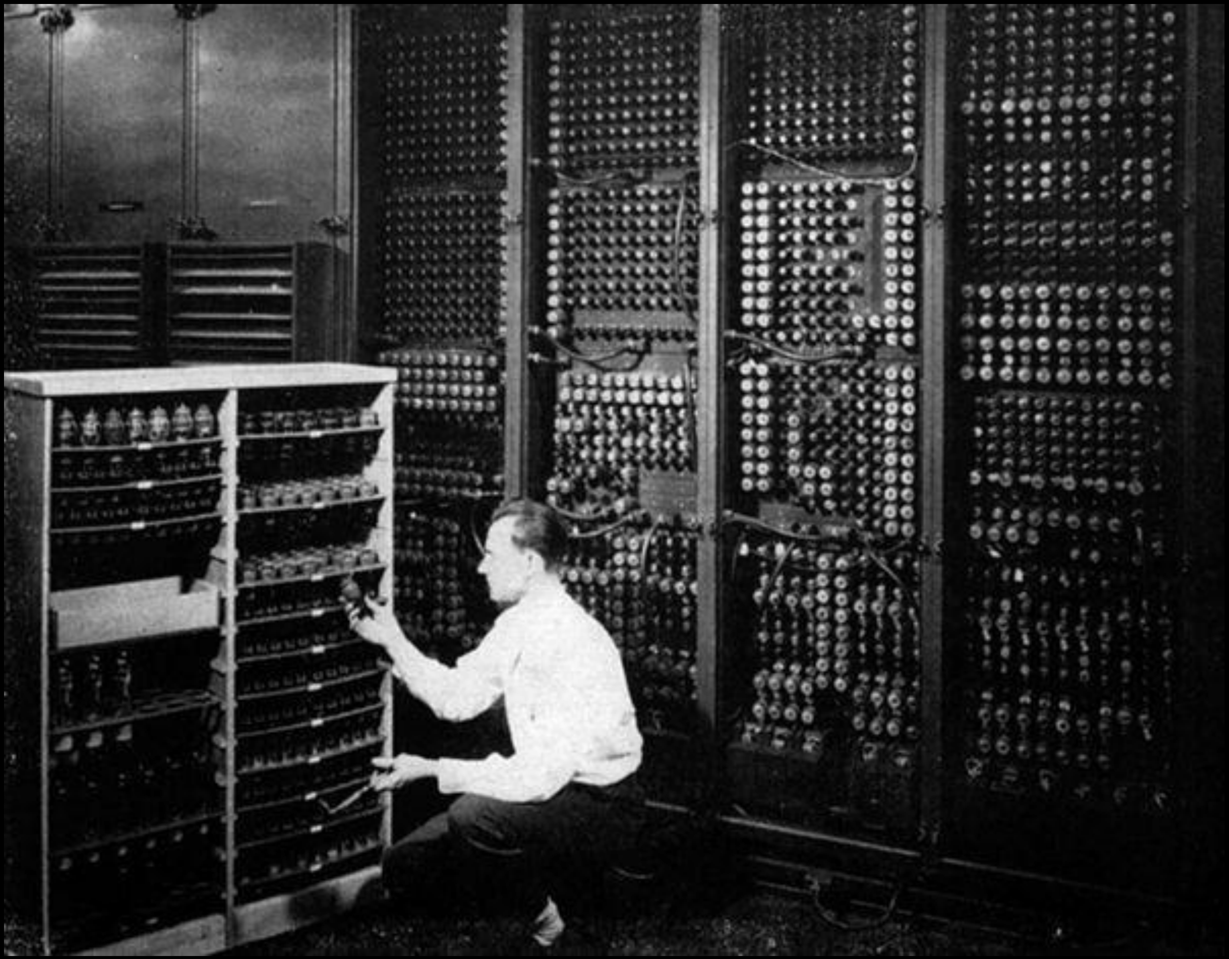


A Brief Intellectual History of Computing

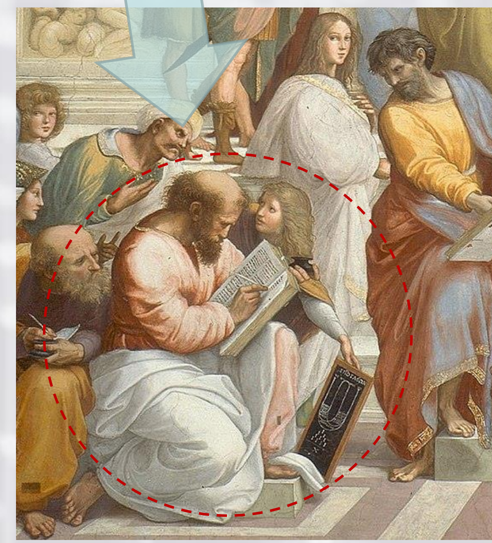
Mathematical (Un)Certainty

- Mathematics is commonly seen as embodying *certainty* – forming the bedrock of most scientific disciplines, and ultimately emblematic of the pinnacle of humanity's intellectual achievements.

- Despite this revered status, the history of mathematics is fraught with instability, and at times its entire edifice has teetered on the brink of total collapse– and along with it, perhaps, the certitude of human knowledge.

- Incredibly, the last widespread assault on mathematical certainty which began at the close of the 19th century, led, in due course, to one of the greatest inventions in our history: **the computer**.

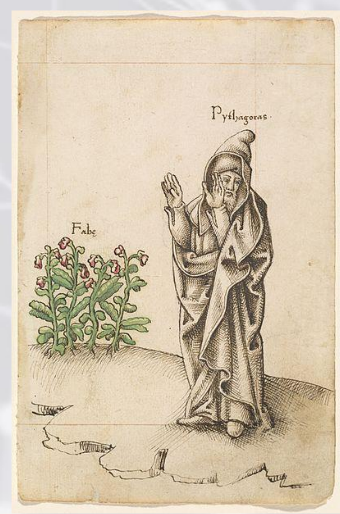
Pythagoras



• One of the first known historical instances of the "**loss of mathematical certainty**" dates to the 5th century BCE and the *cult of Pythagoras* (named for Pythagoras, the ancient Greek philosopher best-known to modern students for the eponymous *Pythagorean Theorem*),

• The philosophy of the Pythagoreans centered around the belief that universe is inherently ordered – and that this order is knowable through natural *laws.*

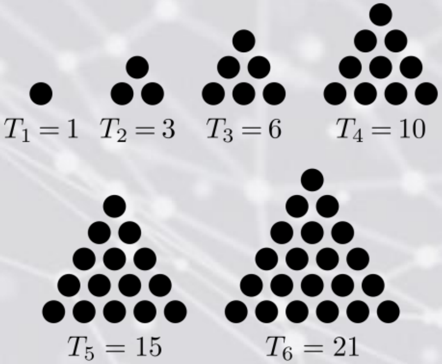
• The Pythagoreans are additionally credited with discovering foundational ideas in music harmony (e.g. absolute intervals); the cult also adhered to vegetarianism, believed in reincarnation, and proposed the notion of the "transmigration of the soul."



Pythagoras

• The Pythagoreans were generally dogmatic mystics; as such, they believed strongly in harmonies discoverable in mathematics (e.g. arithmetic and geometry) as having echoes in broad philosophical and metaphysical concepts, such as *Justice* and *Cosmology*.

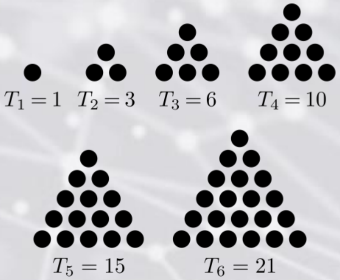
• Numbers were accordingly laden with deep, symbolic meaning. Unconventionally, the Pythagoreans represented numbers graphically; this enabled a visual comprehension of mathematics that dovetailed with geometric concepts.



Pythagoras

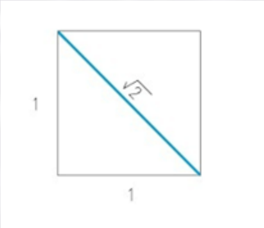
• The Pythagoreans were generally dogmatic mystics; as such, they believed strongly in harmonies discoverable in mathematics (e.g. arithmetic and geometry) as having echoes in broad philosophical and metaphysical concepts, such as *Justice* and *Cosmology*.

• Numbers were accordingly laden with deep, symbolic meaning. Unconventionally, the Pythagoreans represented numbers graphically; this enabled a visual comprehension of mathematics that dovetailed with Geometric concepts.

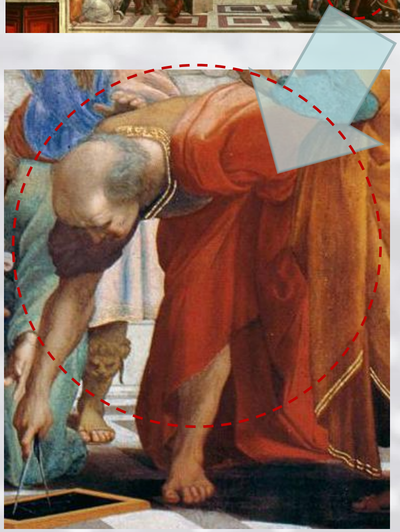


• In the fifth century BCE, Hippasus a disciple of Pythagoras, is said to have provided proof that $\sqrt{2}$ is *irrational* (and hence incommensurable).

• It is alleged (possibly apocryphally) that Hippasus was murdered as a result of this discovery.



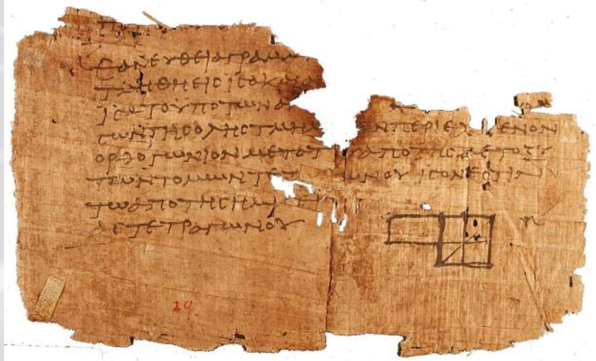
Euclid



• The birth of formal systems of mathematics dates to the third century BCE with Euclid's *Elements* (some say: the most influential textbook every written).

• The *Elements* consists of 13 books, largely covering geometry and number theory; perhaps most significantly, Euclid provides a schematic for a general, "axiomatic approach."

• This approach gives the impression of mathematical certainty: beginning with axioms or postulates, one derives results using logical deductions. <u>If the axioms are true and the logical deductions are valid, then we are guaranteed that the conclusions are likewise true</u>.

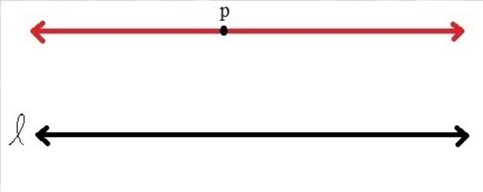


Euclid

• Euclid's demonstration of this axiomatic approach seems to suggest that "new" mathematics (moreover: new <u>knowledge</u>) could be generated – perhaps indefinitely – in this manner.

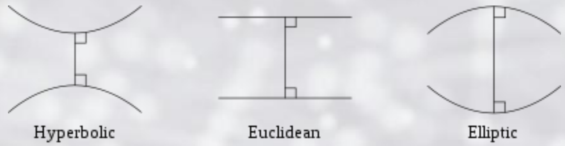
• By the midpoint of the 19th century, however, mathematicians began to discover that this method was flawed. Certain claims (see: *the parallel postulate*) that seemed self-evident by perception could not – despite mathematicians' best efforts – be proven from the axioms.

The parallel postulate states *(paraphrasing):* In a plane, given a line and a point not on it, at most one line parallel to the given line can be drawn through the point.



Euclid

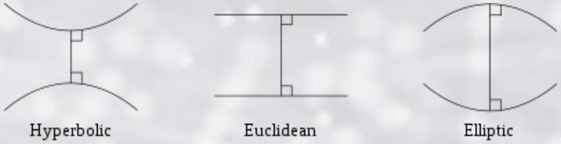
• Interestingly, at this time it was shown that, despite their counter-intuitive nature, **consistent** geometries – <u>non-Euclidean geometries</u> – exist for which the parallel postulate is assumed false.



• This discovery spurred a bona fide paradigm shift – not only in mathematics and logic (as we shall see) – but across all intellectual culture in the 19th century.

Euclid

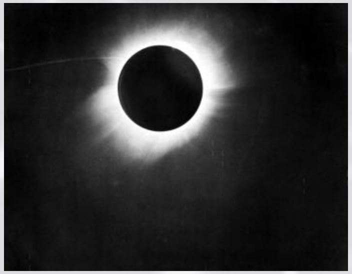
• Interestingly, at this time it was shown that, despite their counter-intuitive nature, **consistent** geometries – non-Euclidean geometries – exist for which the parallel postulate is assumed false.



• This discovery spurred a bona fide paradigm shift – not only in mathematics and logic (as we shall see) – but across all intellectual culture in the 19^{th} century.

• Two giants were seemingly felled at once: (1) mathematical certainty as a whole was called into question and (2) the self-evident notion that the universe was inherently Euclidean now seemed in doubt as well.

• In one of the greatest scientific discoveries in modern history, the observation of the 1919 total solar eclipse which showed that rays of starlight are bent by gravity (as predicted by Einstein's *general theory of relativity*), provided proof, in fact, of the the *non-Euclidean* nature of the universe.



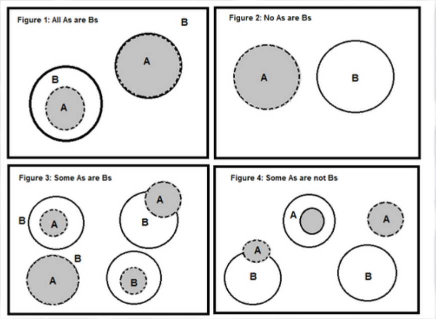
Logic

• Euclid's *Elements* was highly influential not only for its mathematical results, but also for its logical arguments that demonstrated how these results could be obtained from simpler ones.

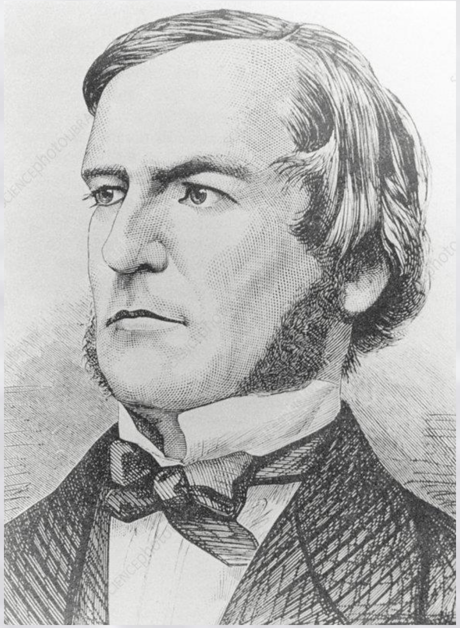
• *Elements* is a text that not only teaches you mathematics, but also how to argue logically.

• As a discipline, **Logic** represents an attempt to codify human "reasoning"; it generally centers on the study of valid forms of *inference*.

• The work of Aristotle (*Organon*) in the 4^{th} century BCE exerted a tremendous influence on the study of Logic from antiquity through the 19^{th} century; in particular, Aristotle's work was influential for its introduction of variables and comprehensive analysis of *syllogistic forms*.

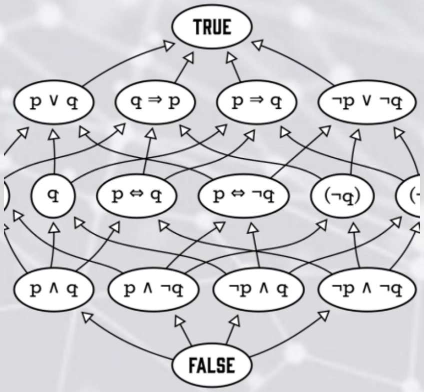


Boole

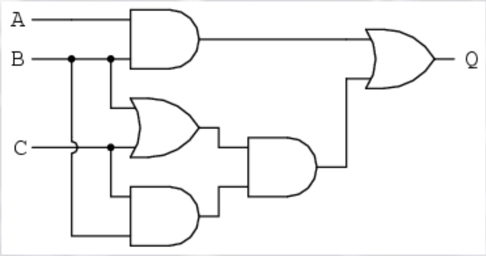


• In the mid 19th century, George Boole established a strong consonance between logic and mathematics. In particular, he determined that logical deductions involving the connectives: **AND**, **OR** and **NOT** could be <u>reduced to algebraic manipulation of symbols</u>.

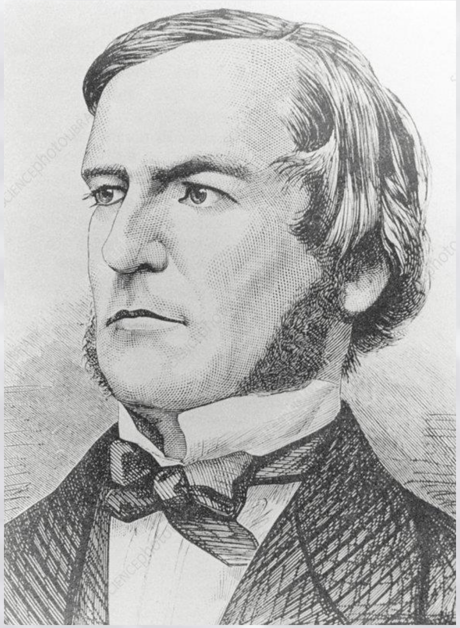
• Boole's results were later extended to encompass a comprehensive system now know as **Boolean algebra**.



• Boolean algebra provides a foundation for logic gates and modern circuit design.



Boole



• Boolean algebra only pertained to **propositional logic** (i.e. *zero-order logic*) – meaning that it didn't include quantifiers such as "all" and "some." Crucially, the logic that underlies the usual foundations of mathematics requires quantifiers – that is to say, it needs be a **first-order logic**.

• For instance, the natural numbers $N = \{1,2,3, \dots\}$ can be described using the so-called first-order *Peano axioms*, which built upon Boole's work:

- $\forall x \; 0 \neq S(x)$
- $\forall x, y \; S(x) = S(y) \implies x = y$
- $\forall x \in \mathbb{N} x + 0 = x$
- $\forall x, y \in \mathbb{N} x + S(y) = S(x + y)$
- $\forall x \in \mathbb{N} x \cdot 0 = 0$
- $\forall x, y \in \mathbb{N} x \cdot S(y) = x \cdot y + x$

• Following the revelation that mathematics could – potentially – be built upon the scaffolding of Logic, many mathematicians and logicians (see: Frege, Peirce) in the second half of the 19th century undertook to build a complete, first-order axiomatic system (à la Euclid) from which all of mathematics could be derived (*Logicism*).

Logic Machines

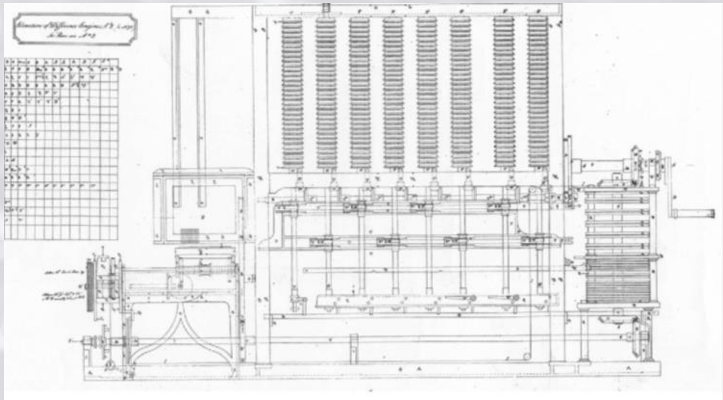
• In part, the interest in solving this grandiose problem stemmed from a centuries-old dream to build a "logic machine" – or better still: an omniscient oracle.

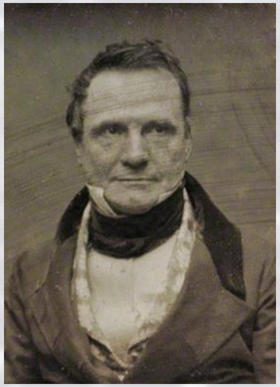
• In the early 17th century, Pascal developed one of the first functioning mechanical calculators (ostensibly it performed addition and subtraction), known today as the *Pascaline*.

• Inspired by Pascal's work, Leibniz later designed the *stepped reckoner*, which could also perform multiplication and division operations.

Logic Machines

• In the early 19th century, Charles Babbage designed the *Difference Engine* which simulated Newton's "Divided Difference" algorithm for computing coefficients of interpolating polynomials.

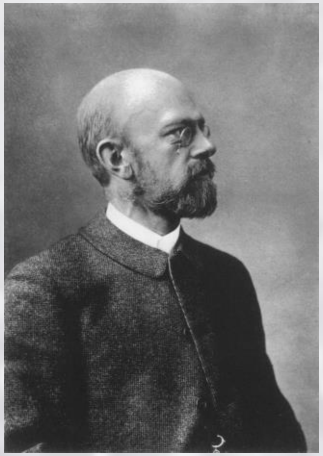




• Babbage later proposed (1837) the *Analytical Engine*, a general-purpose computer (never built due to inadequate funding) that incorporated an arithmetic logic unit, control flow (e.g. for loops) and integrated memory. Note that the first physically-realized, general-purpose computer did not appear until over a century later, in 1941, with the 'Z3' designed by Konrad Zuse.

• Ada Lovelace, considered by some to be the first "programmer" in history, provided extensive notes on the Analytical Engine, including the first published algorithm using the Analytical Engine to compute Bernoulli numbers. Lovelace also wrote precociously regarding the potential limits of logic machines vis-à-vis human creativity, and the bounds of what we today call Artificial Intelligence.

Hilbert



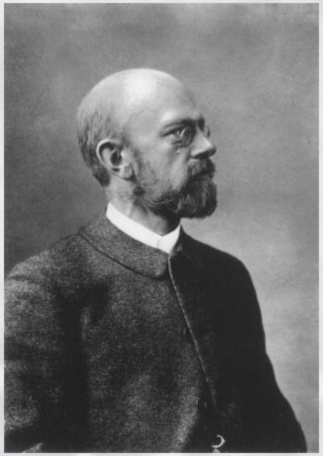
• As mentioned previously, the latter half of the 19th century saw the introduction of various non-Euclidean geometries. Given the primacy given to Euclidean geometry at this time (due to its seemingly natural correspondence with our experience of reality), theorists began to wonder whether these new systems were *consistent*.

• Informally, an axiomatic system is consistent if it lacks **contradiction**, i.e., the ability to derive both a statement and its denial from the axioms of this system. This notion of consistency spawned directly from Aristotle's notion of the **law of the excluded middle**.

• David Hilbert, one of the most influential mathematicians of the last half of the 19th century and early part of the 20th, proved in 1899 that Euclidean geometry was consistent **if** arithmetic was consistent (subsequent mathematicians proved that non-Euclidean geometries were consistent if Euclidean geometry was!).

• From this starting point, much of mathematics in the 20th century evolved into a network of axiomatic formal systems (i.e. *metamathematics*).

Hilbert



• These proofs of relative consistency were comforting, but it was realized that a proof of consistency shouldn't depend on the assumption that another area of mathematics was consistent.

• Instead, what was needed was a proof of *consistency* and *completeness* (meaning that every statement could be either proven or disproven from the axioms) of a foundational axiomatic system for mathematics.

• The idea that mathematics could be built on a system of axioms that were <u>complete, consistent and admitted of a proof of consistency from within the system</u> became known as *Hilbert's Program* (1920).

• In 1928, Hilbert added what is know as the *Entscheidungsproblem* ("**decision problem**") to his program, the problem that asks for an algorithm that takes as input a statement of first-order logic and answers "Yes" or "No" according to whether the statement can be deduced from the axioms. <u>Hilbert was certain that such an algorithm existed</u>.

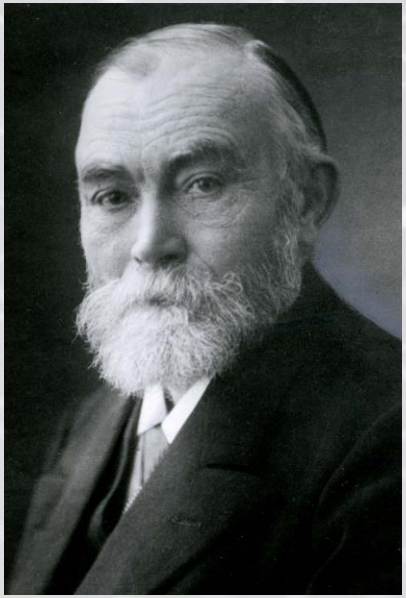
"We must know,
we will know."

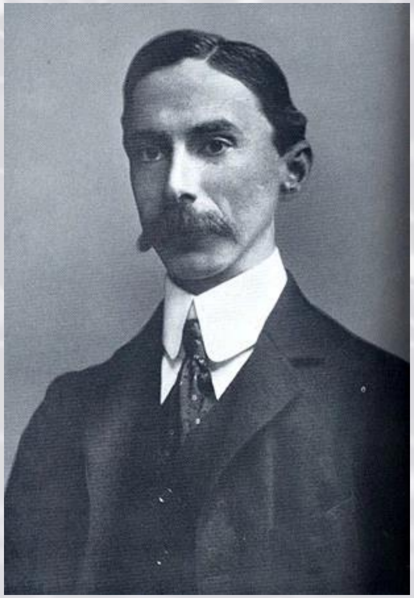
Russell & Whitehead

• In 1902, just as he was about to publish the second volume to his magnum opus (*Basic Laws of Arithmetic*), the German logician Gottlob Frege received a letter from Bertrand Russell informing him of a fundamental paradox lying at the heart of Frege's *theory of sets*.

• The paradox (derivable from Frege's basic laws) concerns the notion of the "set of all sets." The paradox today is known as **Russell's Paradox** (sometimes expressed colloquially as the *Barber Paradox*):

> Consider any definable collection to be a set. Let *R* be <u>the set of all sets that are not members of themselves</u>. If *R* is not a member of itself, then its definition dictates that it must contain itself, and if it contains itself, then it contradicts its own definition as the set of all sets that are not members of themselves.





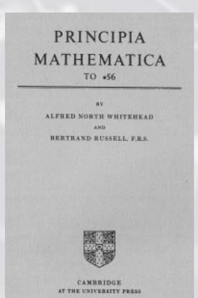
Russell & Whitehead

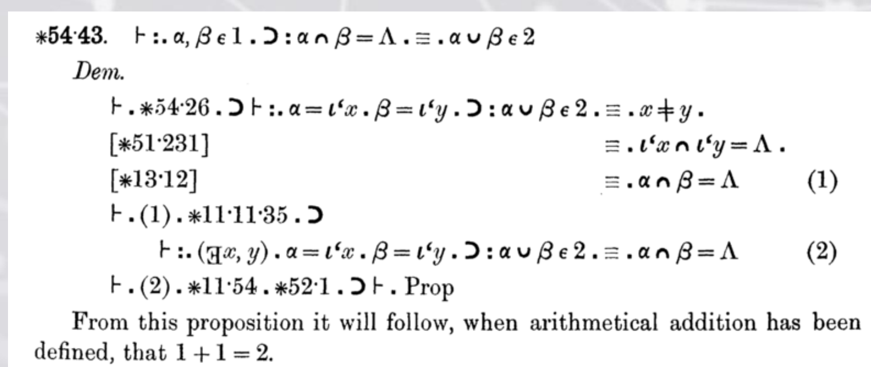
• In spite of the discovery of this paradox, Russell believed that Frege had the right approach and that the flaw could be remedied.

• Russell famously undertook one of the most monumental efforts in the history of mathematics, with Alfred North Whitehead, in writing the massive, three volume *Principia Mathematica.*

• The aim of this work was to once and for all place mathematics on a firm (i.e. an axiomatically <u>consistent and complete</u>) foundation of logic using a minimum of axioms and inference rules.

• This endeavor was notoriously laborious and incorporated the lapidary use of Russell's *theory of types* (to replace sets). Incredibly, it is not until p. 379 of volume 1 that the authors establish the proof of the proposition: 1+1=2. Citing intellectual exhaustion, the authors finally abandoned plans for additional volumes, including the treatment of geometry.




$*54\cdot43.\quad \vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . *54\cdot26 . \supset \vdash :. \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

$[*51\cdot231] \qquad \equiv . \iota`x \cap \iota`y = \Lambda .$

$[*13\cdot12] \qquad \equiv . \alpha \cap \beta = \Lambda \qquad (1)$

$\vdash . (1) . *11\cdot11\cdot35 . \supset$

$\vdash :. (\exists x, y) . \alpha = \iota`x . \beta = \iota`y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \qquad (2)$

$\vdash . (2) . *11\cdot54 . *52\cdot1 . \supset \vdash .$ Prop

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

Gödel

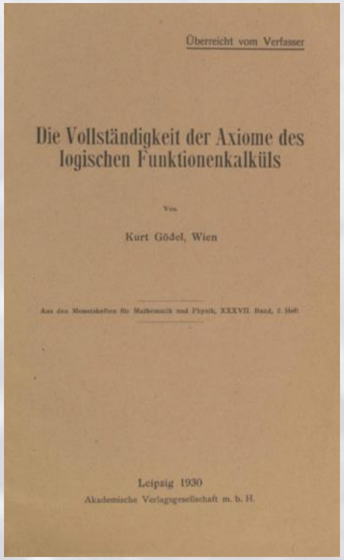
- In 1931, Kurt Gödel published his first (of two) landmark **Incompleteness Theorems**.

In essence, Gödel showed that for systems of axioms that were strong enough to prove results about numbers (e.g. the *Principia*), if the axioms were consistent, then they could not be complete (in this way Gödel "*out-Russelled" Russell*).

- In other words, <u>there would always be statements that could be neither proven nor disproven from the axioms</u>; he additionally showed that it was impossible to prove the consistency of the axioms from within the system itself.

- This result is widely understood to have shown that <u>Hilbert's program for finding a complete and consistent set of axioms for all mathematics is impossible</u> – however, there was still the matter of the resolution of the *Entscheidungsproblem.*

Gödel



- Briefly: How did Gödel prove the first Incompleteness Theorem?

i. Gödel defines an encoding scheme that assigns each symbol in a *well-formed-formula* of some formal language a <u>unique</u> natural number, called its **Gödel number** – this was a highly original and subsequently influential idea at the time (think of ASCII).

$$\mathrm{enc}(x_1, x_2, x_3, \ldots, x_n) = 2^{x_1} \cdot 3^{x_2} \cdot 5^{x_3} \cdots p_n^{x_n}$$

• The significance of this (reversible) encoding scheme was that <u>determining properties of statements (e.g. their truth or falsehood) would be equivalent to determining whether their Gödel numbers had certain properties</u>.

ii. Next, Gödel constructs a statement G "*this statement is not demonstrable in S*" (S is the formal system) akin to the **Liar's Paradox** ("this statement is false"). This implies G iff ~G. Importantly, this indicates that if **if S is consistent, it is necessarily undecidable** (because G iff ~G).

Gödel

i. Gödel defines an encoding scheme that assigns a wff to its Gödel number.

ii. Construct statement G so that: G iff ~G. **We conclude that if S is consistent, then it is undecidable**.

iii. The remarkable aspect of (ii) is that Gödel subsequently shows, **using metamathematical reasoning that G is in fact true**.

Consider, more concretely, the statement G "*this statement is not demonstrable in S*" in the spirit of Gödel's formalism:

$$\sim(\exists x)\,Dem_s(x,z)$$

Where $Dem_S(x,z)$ denotes the claim: for the statements P and Q in S with respective Gödel numbers x and z (i.e. x=enc(P), z=enc(Q)), z is demonstrated using proof x.

• Gödel uses a clever self-reference trick to show that on the level of metamathematics (i.e. relationships between Gödel encodings), <u>the undecidability of G shows that G in fact is not demonstrable in S, meaning that G is true</u>!

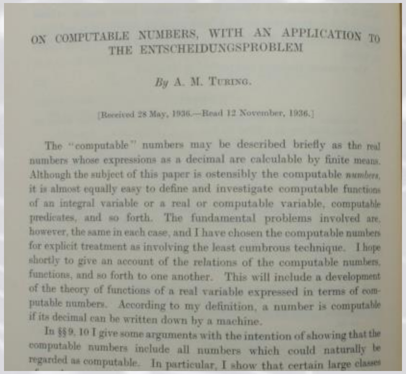
<u>In conclusion</u>: contrary to all prior belief, arithmetical (and moreover, mathematical) truth cannot be brought into systematic order once and for all with a fixed set of axioms and rules for inference from which every true statement can be formally derived.

Turing

• In 1935, while at Cambridge, Turing was exposed to both Gödel's proof and the *Entscheidungsproblem.*

• Strongly influenced by Gödel, Turing was convinced that the assumption underlying the *Entscheidungsproblem* was wrong, and that there was no general, mechanical procedure to decide all problems in mathematics.

• First, though, Turing had to give a formal definition of **computation** and even the notion of an **algorithm** (some contemporaries believed this concept intrinsically eluded formalization), as these concepts had yet to be defined rigorously by the beginning of the 20th century.



ON COMPUTABLE NUMBERS, WITH AN APPLICATION TO THE ENTSCHEIDUNGSPROBLEM

By A. M. TURING.

[Received 28 May, 1936.—Read 12 November, 1936.]

The "computable" numbers may be described briefly as the real numbers whose expressions as a decimal are calculable by finite means. Although the subject of this paper is ostensibly the computable *numbers*, it is almost equally easy to define and investigate computable functions of an integral variable or a real or computable variable, computable predicates, and so forth. The fundamental problems involved are, however, the same in each case, and I have chosen the computable numbers for explicit treatment as involving the least cumbrous technique. I hope shortly to give an account of the relations of the computable numbers, functions, and so forth to one another. This will include a development of the theory of functions of a real variable expressed in terms of computable numbers. According to my definition, a number is computable if its decimal can be written down by a machine.

In §§ 9, 10 I give some arguments with the intention of showing that the computable numbers include all numbers which could naturally be regarded as computable. In particular, I show that certain large classes

• In 1936, Turing published his seminal paper "On Computable Numbers, with an Application to the *Entscheidungsproblem.*" In this paper he formalized the idea of computation (via what we now call **Turing Machines**) and importantly proved the general infeasibility of the *Entscheidungsproblem* by providing several concrete examples of computationally undecidable problems (e.g. the Halting Problem).

*Note that Turing in fact was not the first to prove undecidability, as Alonzo Church proved an equivalent result using *λ-calculus*.

Turing

• Turing's fresh insight was to define algorithms in terms of theoretical computing machines.

• Borrowing from Gödel, Turing devised a procedure to encode machines as binary strings.

• Crucially, using this construction, Turing conceived of a *universal machine* (i.e. a **universal Turing machine**) that could simulate any other Turing machine – the universal machine *UM* could simply ingest both an input string *s* and the encoding of a Turing machine *M* (one could merely concatenate these encodings). In this way, the universal machine could simulate machine *M* running the input *s*.

• Turing uses an argument analogous to Cantor's diagonalization argument to prove that the Halting Problem is undecidable. The gist of this argument has close parallels with arguments provided by Russell and Gödel.

Turing

Sketch of Turing's Proof of the Undecidability of the Halting Problem:

Pf. Suppose not, and so suppose that the Halting is decidable (this form of proof is called *proof by contradiction*). Consequently, we assume that there exists an algorithm halts(·) where halts(f) returns true if subroutine f halts (when run with no inputs) and halts(f) returns false otherwise, in general.

Now define the subroutine *g*:

```
def g():
    if halts(g):
        loop_forever()
```

Consider now what happens when we run halts(*g*). By assumption of the decidability of the Halting Problem, halts(*g*) must return True or False (but not both).

Case 1: If we suppose halts(*g*) is True, then halts(g) runs forever, so halts(*g*) is also False, a <u>contradiction</u>.

Conversely, **Case 2**: If we suppose halts(g) is False, then halts(g) halts, indicating that it is a True, a <u>contradiction</u>.

Because both causes yield a contradiction, <u>**it follows that the Halting problem is undecidable**</u>.

Turing

- Turing's paper can be viewed in two fundamental ways:

(1) It is a paper on the logical foundations of mathematics that helped end Hilbert's program by showing that the *Entscheidungsproblem* was critically flawed.

(2) It can be viewed also as the paper that started the study of the theory of computation and directly ushered in the birth of computer science as a formal discipline, and ultimately directly lead to the dawn of the modern computer age.

Fin