# Some interesting things that do not exist

Dr Richard Smith

(http://maths.ucd.ie/~rsmith)

UCD, 14th October 2015

# Formulae to solve polynomials

## The Quadratic Formula (Babylon . . . al-Khwārizmī c. 830)

If $x^2 + bx + c = 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

# Formulae to solve polynomials

## The Quadratic Formula (Babylon . . . al-Khwārizmī c. 830)

If $x^2 + bx + c = 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

## The Cubic Formula (Cardano, Tartaglia 1545)

If $x^3 + bx^2 + cx + d = 0$, then

# Formulae to solve polynomials

## The Quadratic Formula (Babylon . . . al-Khwārizmī c. 830)

If $x^2 + bx + c = 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

## The Cubic Formula (Cardano, Tartaglia 1545)

If $x^3 + bx^2 + cx + d = 0$, then

$$x = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}} - \frac{b}{3} \dots$$

# Formulae to solve polynomials

## The Quadratic Formula (Babylon . . . al-Khwārizmī c. 830)

If $x^2 + bx + c = 0$, then

$$x = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

## The Cubic Formula (Cardano, Tartaglia 1545)

If $x^3 + bx^2 + cx + d = 0$, then

$$x = \sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}} - \frac{b}{3} \ldots$$

. . . where $p = \dfrac{3c - b^2}{3}$ and $q = \dfrac{2b^3 - 9bc + 27d}{27}$.

# Formulae to solve polynomials

## The Quartic Formula (Ferrari 1545)

If $x^4 + bx^3 + cx^2 + dx + e = 0$, then

$$x = \pm\sqrt{\frac{u}{2}} \pm \sqrt{-\frac{u}{2} - \frac{p}{2} - \frac{\pm q}{2\sqrt{2u}}} + \frac{b}{4},$$

# Formulae to solve polynomials

## The Quartic Formula (Ferrari 1545)

If $x^4 + bx^3 + cx^2 + dx + e = 0$, then

$$x = \pm\sqrt{\frac{u}{2}} \pm \sqrt{-\frac{u}{2} - \frac{p}{2} - \frac{\pm q}{2\sqrt{2u}}} + \frac{b}{4},$$

where $p = \dfrac{16c - 6b^2}{16}$, $q = \dfrac{8d - 4bc + b^3}{8}$, $r = \dfrac{256e - 64bd + 16b^2c - 3b^4}{256}$,

# Formulae to solve polynomials

## The Quartic Formula (Ferrari 1545)

If $x^4 + bx^3 + cx^2 + dx + e = 0$, then

$$x = \pm\sqrt{\frac{u}{2}} \pm \sqrt{-\frac{u}{2} - \frac{p}{2} - \frac{\pm q}{2\sqrt{2u}}} + \frac{b}{4},$$

where $p = \dfrac{16c - 6b^2}{16}$, $q = \dfrac{8d - 4bc + b^3}{8}$, $r = \dfrac{256e - 64bd + 16b^2c - 3b^4}{256}$,

...and $u$ is a solution of the cubic equation

$$8u^3 + 8pu^2 + (2p^2 - 8r)u - q^2 = 0$$

# Formulae to solve polynomials

## The Quartic Formula (Ferrari 1545)

If $x^4 + bx^3 + cx^2 + dx + e = 0$, then

$$x = \pm\sqrt{\frac{u}{2}} \pm \sqrt{-\frac{u}{2} - \frac{p}{2} - \frac{\pm q}{2\sqrt{2u}}} + \frac{b}{4},$$

where $p = \dfrac{16c - 6b^2}{16}$, $q = \dfrac{8d - 4bc + b^3}{8}$, $r = \dfrac{256e - 64bd + 16b^2c - 3b^4}{256}$,

…and $u$ is a solution of the cubic equation

$$8u^3 + 8pu^2 + (2p^2 - 8r)u - q^2 = 0$$

…**and** provided $q \neq 0$!

# Formulae to solve polynomials

## The Quartic Formula (Ferrari 1545)

If $x^4 + bx^3 + cx^2 + dx + e = 0$, then

$$x = \pm\sqrt{\frac{u}{2}} \pm \sqrt{-\frac{u}{2} - \frac{p}{2} - \frac{\pm q}{2\sqrt{2u}}} + \frac{b}{4},$$

where $p = \dfrac{16c - 6b^2}{16}$, $q = \dfrac{8d - 4bc + b^3}{8}$, $r = \dfrac{256e - 64bd + 16b^2c - 3b^4}{256}$,

...and $u$ is a solution of the cubic equation

$$8u^3 + 8pu^2 + (2p^2 - 8r)u - q^2 = 0$$

...**and** provided $q \neq 0$! If $q = 0$, then

$$x = \pm\sqrt{-\frac{p}{2} \pm \sqrt{\left(\frac{p}{2}\right)^2 - r}} + \frac{b}{4}.$$

# A Quintic Formula?

So what if we have a **quintic equation**

$$x^5 + bx^4 + cx^3 + dx^2 + ex + f = 0? \tag{1}$$

# A Quintic Formula?

So what if we have a **quintic equation**

$$x^5 + bx^4 + cx^3 + dx^2 + ex + f = 0? \tag{1}$$

**Theorem (Abel 1824)**

'There is no quintic formula, and there never will be.'

# A Quintic Formula?

So what if we have a **quintic equation**

$$x^5 + bx^4 + cx^3 + dx^2 + ex + f = 0? \tag{1}$$

**Theorem (Abel 1824)**

'There is no quintic formula, and there never will be.'

This does NOT mean that quintic equations have no solutions!

# A Quintic Formula?

So what if we have a **quintic equation**

$$x^5 + bx^4 + cx^3 + dx^2 + ex + f \;=\; 0? \tag{1}$$

**Theorem (Abel 1824)**

'There is no quintic formula, and there never will be.'

This does NOT mean that quintic equations have no solutions!

The quintic equation

$$x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1 \;=\; 0$$

has unique solution $x = 1$.

# A Quintic Formula?

So what if we have a **quintic equation**

$$x^5 + bx^4 + cx^3 + dx^2 + ex + f = 0? \tag{1}$$

**Theorem (Abel 1824)**

'There is no quintic formula, and there never will be.'

This does NOT mean that quintic equations have no solutions!

The quintic equation

$$x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1 = 0$$

has unique solution $x = 1$.

Moreover, by the **Fundamental Theorem of Algebra**, equation (1) above **always** has between 1 and 5 distinct solutions (some possibly in $\mathbb{C}$).

# When are you a radical?

We must clarify what we mean by ‘formula’.

# When are you a radical?

We must clarify what we mean by ‘formula’.

## Radical expressions

Consider the equation

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots a_1 x + a_0 \; = \; 0,$$

where the coefficients $a_0, a_1, \ldots a_{n-1} \in \mathbb{Q}$ are rational.

# When are you a radical?

We must clarify what we mean by 'formula'.

## Radical expressions

Consider the equation

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots a_1 x + a_0 = 0,$$

where the coefficients $a_0, a_1, \dots a_{n-1} \in \mathbb{Q}$ are rational.

A **radical expression** (over $\mathbb{Q}$) is a quantity that can be built up from the coefficients $a_0, a_1, \dots, a_{n-1}$, by applying the operations $+$, $-$, $\times$, $/$, and also $n$th roots $\sqrt{\ }$, $\sqrt[3]{\ }$, $\sqrt[4]{\ }$, ....

# When are you a radical?

We must clarify what we mean by ‘formula’.

## Radical expressions

Consider the equation

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots a_1 x + a_0 \;=\; 0,$$

where the coefficients $a_0, a_1, \dots a_{n-1} \in \mathbb{Q}$ are rational.

A **radical expression** (over $\mathbb{Q}$) is a quantity that can be built up from the coefficients $a_0, a_1, \dots, a_{n-1}$, by applying the operations $+$, $-$, $\times$, $/$, and also $n$th roots $\sqrt{\ }$, $\sqrt[3]{\ }$, $\sqrt[4]{\ }$, ....

The existence of the quadratic formula implies that the solutions of every quadratic equation with rational coefficients are radical expressions.

# When are you a radical?

We must clarify what we mean by ‘formula’.

## Radical expressions

Consider the equation

$$x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots a_1 x + a_0 \;=\; 0,$$

where the coefficients $a_0, a_1, \dots a_{n-1} \in \mathbb{Q}$ are rational.

A **radical expression** (over $\mathbb{Q}$) is a quantity that can be built up from the coefficients $a_0, a_1, \dots, a_{n-1}$, by applying the operations $+$, $-$, $\times$, $/$, and also $n$th roots $\sqrt{\ }$, $\sqrt[3]{\ }$, $\sqrt[4]{\ }$, ....

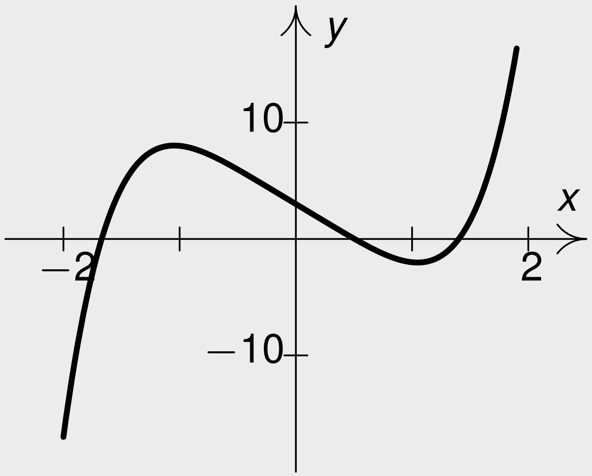
The existence of the quadratic formula implies that the solutions of every quadratic equation with rational coefficients are radical expressions. Likewise for the cubic and quartic formulae.

# There is no quintic formula

If a quintic formula existed, then the solutions of every quintic equation with rational coefficients would be radical expressions.

## Example

Consider the quintic equation $x^5 - 6x + 3 = 0$.

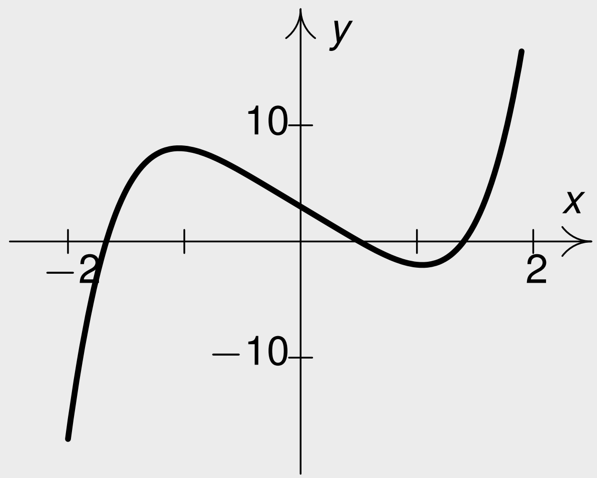


# There is no quintic formula

If a quintic formula existed, then the solutions of every quintic equation with rational coefficients would be radical expressions.

## Example

Consider the quintic equation $x^5 - 6x + 3 = 0$.



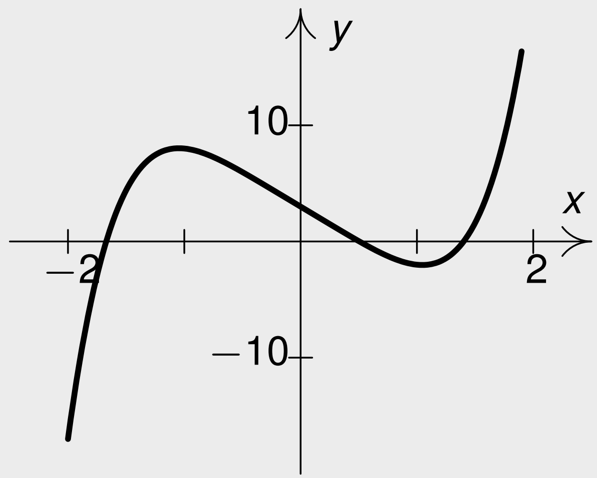

None of the three real solutions of this equation are radical expressions. Thus there is no quintic formula.

# There is no quintic formula

If a quintic formula existed, then the solutions of every quintic equation with rational coefficients would be radical expressions.

## Example

Consider the quintic equation $x^5 - 6x + 3 = 0$.

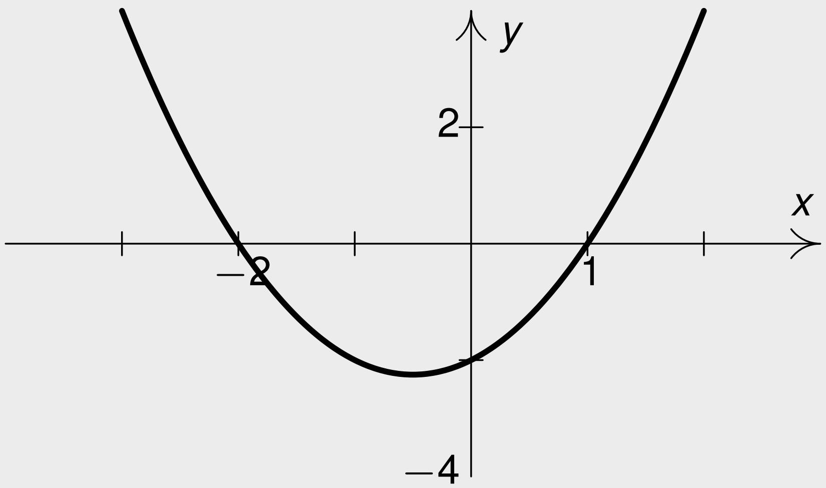



None of the three real solutions of this equation are radical expressions. Thus there is no quintic formula. Nowadays this is proved using **Galois Theory**.

# Polynomial equations with integer solutions

## Example

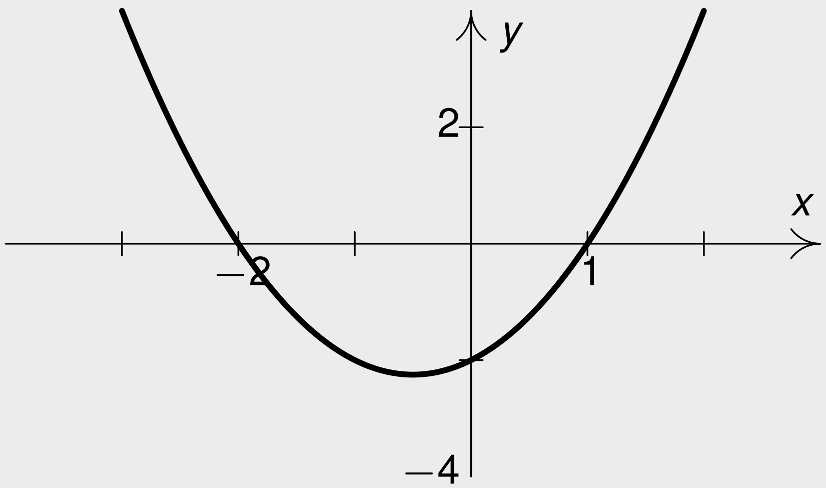
Consider the quadratic equation $x^2 + x - 2 = 0$.



# Polynomial equations with integer solutions

## Example

Consider the quadratic equation $x^2 + x - 2 = 0$.

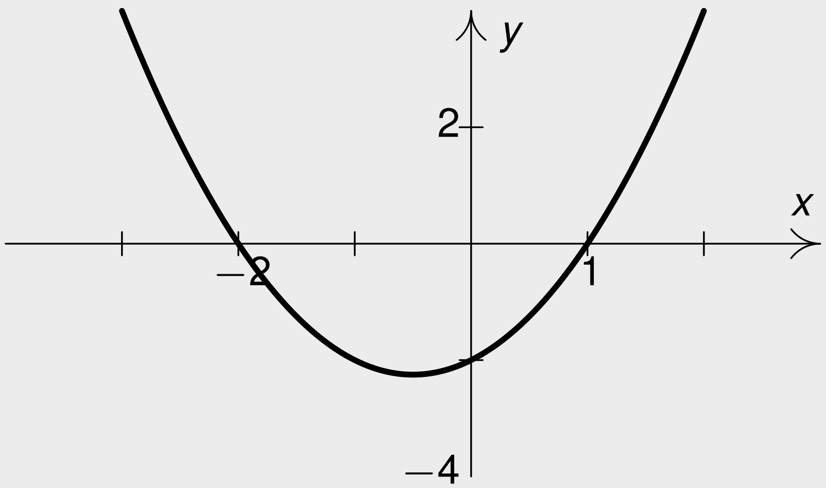



This equation has solutions $x = -2$ and $x = 1$.

# Polynomial equations with integer solutions

## Example

Consider the quadratic equation $x^2 + x - 2 = 0$.



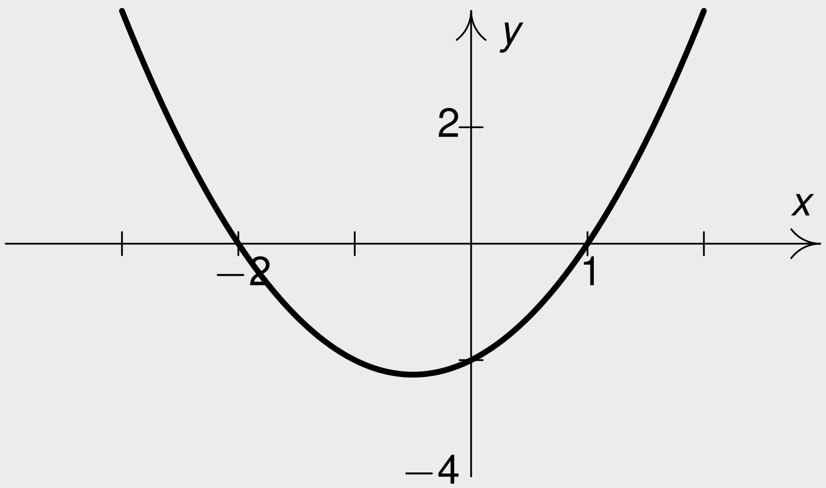

This equation has solutions $x = -2$ and $x = 1$.

However, if $4x^2 - 4x - 15 = 0$, then $x = -\frac{3}{2}$ or $x = \frac{5}{2}$, so no **integer** solutions.

# Polynomial equations with integer solutions

## Example

Consider the quadratic equation $x^2 + x - 2 = 0$.




This equation has solutions $x = -2$ and $x = 1$.

However, if $4x^2 - 4x - 15 = 0$, then $x = -\frac{3}{2}$ or $x = \frac{5}{2}$, so no **integer** solutions.

We can consider equations in several variables too. E.g. $x^2 + y^2 - z^2 = 0$ has infinitely many integer solutions (**Pythagorean triples**).

# Diophantine equations

# Diophantine equations

## Diophantine equations

Let $p(x_1, x_2, \ldots, x_n)$ be a polynomial with integer coefficients. Then

$$p(x_1, x_2, \ldots, x_n) \; = \; 0,$$

for which **integer solutions** are sought is called a **Diophantine equation**.

# Diophantine equations

## Diophantine equations

Let $p(x_1, x_2, \ldots, x_n)$ be a polynomial with integer coefficients. Then

$$p(x_1, x_2, \ldots, x_n) = 0,$$

for which **integer solutions** are sought is called a **Diophantine equation**.

Diophantine equations were introduced Diophantus of Alexandria, 3rd century AD, and have been studied for hundreds of years.

# Diophantine equations

## Diophantine equations

Let $p(x_1, x_2, \ldots, x_n)$ be a polynomial with integer coefficients. Then

$$p(x_1, x_2, \ldots, x_n) = 0,$$

for which **integer solutions** are sought is called a **Diophantine equation**.

Diophantine equations were introduced Diophantus of Alexandria, 3rd century AD, and have been studied for hundreds of years. They can be hard to solve...

# Diophantine equations

## Diophantine equations

Let $p(x_1, x_2, \ldots, x_n)$ be a polynomial with integer coefficients. Then

$$p(x_1, x_2, \ldots, x_n) \;=\; 0,$$

for which **integer solutions** are sought is called a **Diophantine equation**.

Diophantine equations were introduced Diophantus of Alexandria, 3rd century AD, and have been studied for hundreds of years. They can be hard to solve...

## Fermat's Last Theorem (Fermat 1637 (?!), Wiles 95)

Let $k \geq 3$. Then the equation

$$x^k + y^k - z^k \;=\; 0$$

has no (positive) integer solutions in $x$, $y$ and $z$.

# Diophantine equations are very hard to solve. . .

The importance of solving Diophantine equations prompted Hilbert to include it in his famous list of 23 unsolved problems, published in 1900.

# Diophantine equations are very hard to solve. . .

The importance of solving Diophantine equations prompted Hilbert to include it in his famous list of 23 unsolved problems, published in 1900.

## Hilbert's 10th Problem (1900)

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: **To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.**

# Diophantine equations are very hard to solve...

The importance of solving Diophantine equations prompted Hilbert to include it in his famous list of 23 unsolved problems, published in 1900.

## Hilbert's 10th Problem (1900)

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: **To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.**

In today's language: is there is an algorithm or computer program which can, upon input of any polynomial $p(x_1, \ldots, x_n)$ with integer coefficients, determine whether $p(x_1, \ldots, x_n) = 0$ has an integer solution or not?

# Diophantine equations are very hard to solve. . .

The importance of solving Diophantine equations prompted Hilbert to include it in his famous list of 23 unsolved problems, published in 1900.

## Hilbert's 10th Problem (1900)

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: **To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.**

In today's language: is there is an algorithm or computer program which can, upon input of any polynomial $p(x_1, \dots, x_n)$ with integer coefficients, determine whether $p(x_1, \dots, x_n) = 0$ has an integer solution or not?

## Theorem (Matiyasevich 70)

No such algorithm exists!

# Turing Machines

Turing machines are simple abstract computers, introduced at around the same time by Alan Turing and Emil Post in 1936, to formalise the notion of 'algorithm'.

# Turing Machines

Turing machines are simple abstract computers, introduced at around the same time by Alan Turing and Emil Post in 1936, to formalise the notion of 'algorithm'.

Turing machines have two main parts: a memory (the input/output device) and a processor.

# Turing Machines

Turing machines are simple abstract computers, introduced at around the same time by Alan Turing and Emil Post in 1936, to formalise the notion of ‘algorithm’.

Turing machines have two main parts: a memory (the input/output device) and a processor.

The memory can be regarded as an infinite tape, divided up into cells, each containing either 0 or 1.

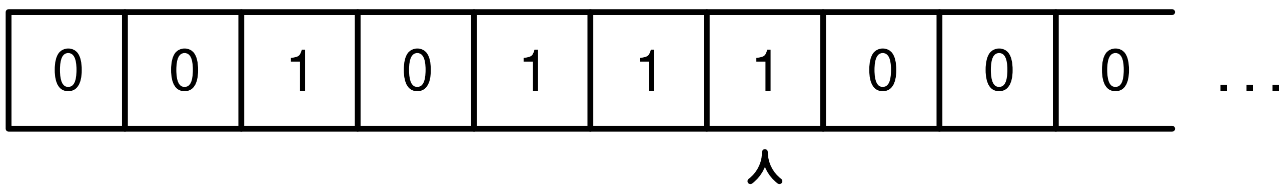
| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | ... |

# Turing Machines

Turing machines are simple abstract computers, introduced at around the same time by Alan Turing and Emil Post in 1936, to formalise the notion of ‘algorithm’.

Turing machines have two main parts: a memory (the input/output device) and a processor.

The memory can be regarded as an infinite tape, divided up into cells, each containing either 0 or 1.



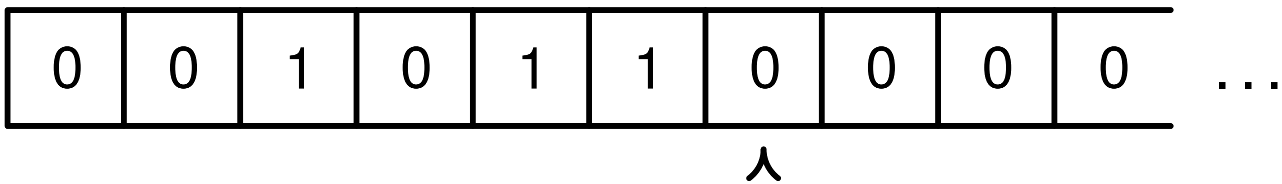

The processor has a scanner which can read from or write to a single cell of the tape at a time, and which moves to the left or right one cell at a time.

# Turing Machines

Turing machines are simple abstract computers, introduced at around the same time by Alan Turing and Emil Post in 1936, to formalise the notion of 'algorithm'.

Turing machines have two main parts: a memory (the input/output device) and a processor.

The memory can be regarded as an infinite tape, divided up into cells, each containing either 0 or 1.




The processor has a scanner which can read from or write to a single cell of the tape at a time, and which moves to the left or right one cell at a time.

# Turing Machines

Turing machines are simple abstract computers, introduced at around the same time by Alan Turing and Emil Post in 1936, to formalise the notion of 'algorithm'.

Turing machines have two main parts: a memory (the input/output device) and a processor.

The memory can be regarded as an infinite tape, divided up into cells, each containing either 0 or 1.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | ... |

The processor has a scanner which can read from or write to a single cell of the tape at a time, and which moves to the left or right one cell at a time.

# Turing machines as computers

## The **successor** machine *S*

| $S$ | 0 | 1 |
|---|---|---|
| 0 | $0R1$ | |
| 1 | $1L2$ | $1R1$ |
| 2 | | $1L2$ |

# Turing machines as computers

## The **successor** machine *S*

| $S$ | 0 | 1 |
|---|---|---|
| 0 | $0R1$ | |
| 1 | $1L2$ | $1R1$ |
| 2 | | $1L2$ |

Given an input tape of the form

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | ... |

# Turing machines as computers

## The **successor** machine $S$

| $S$ | 0 | 1 |
|---|---|---|
| 0 | $0R1$ | |
| 1 | $1L2$ | $1R1$ |
| 2 | | $1L2$ |

Given an input tape of the form

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | ... |

$S$ returns the output tape

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | ... |

# Turing machines as computers

## The **successor** machine $S$

| $S$ | 0 | 1 |
|---|---|---|
| 0 | $0R1$ | |
| 1 | $1L2$ | $1R1$ |
| 2 | | $1L2$ |

In general, $S$ computes the **successor function**

$$n \mapsto n+1.$$

# The Church-Turing Thesis

Despite the fact that Turing machines are extremely rudimentary objects, there is overwhelming evidence to support the following statement. . .

# The Church-Turing Thesis

Despite the fact that Turing machines are extremely rudimentary objects, there is overwhelming evidence to support the following statement. . .

## The Church-Turing Thesis

Given any function

$$f : \mathbb{N}^k \to \mathbb{N}$$

that is **computable by algorithm**, there is a Turing machine that computes $f$.

# The Church-Turing Thesis

Despite the fact that Turing machines are extremely rudimentary objects, there is overwhelming evidence to support the following statement. . .

## The Church-Turing Thesis

Given any function

$$f : \mathbb{N}^k \to \mathbb{N}$$

that is **computable by algorithm**, there is a Turing machine that computes $f$.

## Two computable functions

1. The addition function $(n, m) \mapsto n + m$ is computable by a Turing machine.

# The Church-Turing Thesis

Despite the fact that Turing machines are extremely rudimentary objects, there is overwhelming evidence to support the following statement. . .

## The Church-Turing Thesis

Given any function

$$f : \mathbb{N}^k \to \mathbb{N}$$

that is **computable by algorithm**, there is a Turing machine that computes $f$.

## Two computable functions

1. The addition function $(n, m) \mapsto n + m$ is computable by a Turing machine.
2. The function that returns the $n$th digit of $\pi$ is computable by a Turing machine.

# Turing's Halting Problem

**Theorem (Turing 36)**

There is a well-defined function $h : \mathbb{N} \to \mathbb{N}$ that is not computable by algorithm.

# Turing's Halting Problem

## Theorem (Turing 36)

There is a well-defined function $h : \mathbb{N} \to \mathbb{N}$ that is not computable by algorithm.

There is an algorithm that assigns to each $n \in \mathbb{N}$ a Turing machine $T_n$,

# Turing's Halting Problem

## Theorem (Turing 36)

There is a well-defined function $h : \mathbb{N} \to \mathbb{N}$ that is not computable by algorithm.

There is an algorithm that assigns to each $n \in \mathbb{N}$ a Turing machine $T_n$, such that the list $T_0, T_1, T_2, T_3, \ldots$ contains **all** Turing machines.

# Turing's Halting Problem

## Theorem (Turing 36)

There is a well-defined function $h : \mathbb{N} \to \mathbb{N}$ that is not computable by algorithm.

There is an algorithm that assigns to each $n \in \mathbb{N}$ a Turing machine $T_n$, such that the list $T_0, T_1, T_2, T_3, \ldots$ contains **all** Turing machines.

Define

$$h(n) = \begin{cases} 0 & \text{if } T_n \textbf{ halts}\text{, given input } n \\ 1 & \text{if } T_n \textbf{ does not halt}\text{, given input } n \end{cases}$$

# Turing's Halting Problem

## Theorem (Turing 36)

There is a well-defined function $h : \mathbb{N} \to \mathbb{N}$ that is not computable by algorithm.

There is an algorithm that assigns to each $n \in \mathbb{N}$ a Turing machine $T_n$, such that the list $T_0, T_1, T_2, T_3, \ldots$ contains **all** Turing machines.

Define

$$h(n) = \begin{cases} 0 & \text{if } T_n \textbf{ halts}\text{, given input } n \\ 1 & \text{if } T_n \textbf{ does not halt}\text{, given input } n \end{cases}$$

If $h$ were computable then, by the Church-Turing Thesis, it would be computable by some Turing machine $M$.

# Turing's Halting Problem

## Theorem (Turing 36)

There is a well-defined function $h : \mathbb{N} \to \mathbb{N}$ that is not computable by algorithm.

There is an algorithm that assigns to each $n \in \mathbb{N}$ a Turing machine $T_n$, such that the list $T_0, T_1, T_2, T_3, \ldots$ contains **all** Turing machines.

Define

$$h(n) = \begin{cases} 0 & \text{if } T_n \textbf{ halts}\text{, given input } n \\ 1 & \text{if } T_n \textbf{ does not halt}\text{, given input } n \end{cases}$$

If $h$ were computable then, by the Church-Turing Thesis, it would be computable by some Turing machine $M$. There is a machine that **loops forever** given input 0, and **halts** given input 1.

# Turing's Halting Problem

## Theorem (Turing 36)

There is a well-defined function $h : \mathbb{N} \to \mathbb{N}$ that is not computable by algorithm.

There is an algorithm that assigns to each $n \in \mathbb{N}$ a Turing machine $T_n$, such that the list $T_0, T_1, T_2, T_3, \ldots$ contains **all** Turing machines.

Define

$$h(n) = \begin{cases} 0 & \text{if } T_n \textbf{ halts}\text{, given input } n \\ 1 & \text{if } T_n \textbf{ does not halt}\text{, given input } n \end{cases}$$

If $h$ were computable then, by the Church-Turing Thesis, it would be computable by some Turing machine $M$. There is a machine that **loops forever** given input 0, and **halts** given input 1. We combine machines to get $T$ which

$$\begin{array}{rcl} \textbf{loops forever} \text{ given input } n & \text{if} & T_n \textbf{ halts} \text{ given input } n \\ \textbf{halts} \text{ given input } n & \text{if} & T_n \textbf{ does not halt} \text{ given input } n. \end{array}$$

# Applications of the Halting Problem

We return to the Diophantine problem . . .

# Applications of the Halting Problem

We return to the Diophantine problem . . .

**Theorem (Matiyasevich 70)**

If there is an algorithm that solves all Diophantine equations, then Turing's halting function $h$ above is computable by algorithm.

# Applications of the Halting Problem

We return to the Diophantine problem . . .

**Theorem (Matiyasevich 70)**

If there is an algorithm that solves all Diophantine equations, then Turing's halting function $h$ above is computable by algorithm.

But Turing tells that $h$ is **not** computable by algorithm, so there is no such Diophantine algorithm!

# Applications of the Halting Problem

We return to the Diophantine problem . . .

**Theorem (Matiyasevich 70)**

If there is an algorithm that solves all Diophantine equations, then Turing's halting function $h$ above is computable by algorithm.

But Turing tells that $h$ is **not** computable by algorithm, so there is no such Diophantine algorithm!

**There is no universal debugging program**

There can **never** be a computer program which can automatically debug any computer program that it receives as input.

# Applications of the Halting Problem

We return to the Diophantine problem . . .

**Theorem (Matiyasevich 70)**

If there is an algorithm that solves all Diophantine equations, then Turing's halting function $h$ above is computable by algorithm.

But Turing tells that $h$ is **not** computable by algorithm, so there is no such Diophantine algorithm!

**There is no universal debugging program**

There can **never** be a computer program which can automatically debug any computer program that it receives as input.

This is **even** assuming arbitrary storage capacity or execution time!

# What is true and what is false?

To a mathematician, a mathematical statement is **true** if it can be proved, and **false** if its negation can be proved.

# What is true and what is false?

To a mathematician, a mathematical statement is **true** if it can be proved, and **false** if its negation can be proved.

## Two mathematical statements

The number $\sqrt{2}$ is irrational.

There are only finitely many prime numbers.

# What is true and what is false?

To a mathematician, a mathematical statement is **true** if it can be proved, and **false** if its negation can be proved.

## Two mathematical statements

The number $\sqrt{2}$ is irrational.

There are only finitely many prime numbers.

The first statement is true because it can be proved.

# What is true and what is false?

To a mathematician, a mathematical statement is **true** if it can be proved, and **false** if its negation can be proved.

## Two mathematical statements

The number $\sqrt{2}$ is irrational.

There are only finitely many prime numbers.

The first statement is true because it can be proved.

The second statement is false because its negation can be proved.

# What is true and what is false?

To a mathematician, a mathematical statement is **true** if it can be proved, and **false** if its negation can be proved.

## Two mathematical statements

The number $\sqrt{2}$ is irrational.

There are only finitely many prime numbers.

The first statement is true because it can be proved.

The second statement is false because its negation can be proved.

Properly formulated mathematical statements are **absolutely precise**: the statements contain no ambiguities which might confuse their truth or otherwise.

# What is true and what is false?

To a mathematician, a mathematical statement is **true** if it can be proved, and **false** if its negation can be proved.

## Two mathematical statements

The number $\sqrt{2}$ is irrational.

There are only finitely many prime numbers.

The first statement is true because it can be proved.

The second statement is false because its negation can be proved.

Properly formulated mathematical statements are **absolutely precise**: the statements contain no ambiguities which might confuse their truth or otherwise.

Given their precision, it is reasonable to assume that any given mathematical statement can be proved to be true or false, given sufficient time and effort.

# The Continuum Hypothesis (CH)

## Hilbert's 1st Problem (1900)

Let $E$ be an **uncountable** set of real numbers. Is there a bijection

$$f : E \to \mathbb{R}?$$

# The Continuum Hypothesis (CH)

## Hilbert's 1st Problem (1900)

Let $E$ be an **uncountable** set of real numbers. Is there a bijection

$$f : E \to \mathbb{R}?$$

The Continuum Hypothesis (CH) asserts that Hilbert's 1st problem has a positive solution: if $E$ is uncountable then a bijection $f : E \to \mathbb{R}$ exists.

# The Continuum Hypothesis (CH)

## Hilbert's 1st Problem (1900)

Let $E$ be an **uncountable** set of real numbers. Is there a bijection

$$f : E \to \mathbb{R}?$$

The Continuum Hypothesis (CH) asserts that Hilbert's 1st problem has a positive solution: if $E$ is uncountable then a bijection $f : E \to \mathbb{R}$ exists.

## Theorem (Gödel 40)

There is no **proof** of the **negation** of CH.

# The Continuum Hypothesis (CH)

## Hilbert's 1st Problem (1900)

Let $E$ be an **uncountable** set of real numbers. Is there a bijection

$$f : E \to \mathbb{R}?$$

The Continuum Hypothesis (CH) asserts that Hilbert's 1st problem has a positive solution: if $E$ is uncountable then a bijection $f : E \to \mathbb{R}$ exists.

## Theorem (Gödel 40)

There is no **proof** of the **negation** of CH.

In other words, we cannot **prove** that CH is false. So CH must be true, right?

# The Continuum Hypothesis (CH)

## Hilbert's 1st Problem (1900)

Let $E$ be an **uncountable** set of real numbers. Is there a bijection

$$f : E \to \mathbb{R}?$$

The Continuum Hypothesis (CH) asserts that Hilbert's 1st problem has a positive solution: if $E$ is uncountable then a bijection $f : E \to \mathbb{R}$ exists.

## Theorem (Gödel 40)

There is no **proof** of the **negation** of CH.

In other words, we cannot **prove** that CH is false. So CH must be true, right?

## Theorem (Cohen 63)

There is no proof of CH.

# The Continuum Hypothesis (CH)

## Hilbert's 1st Problem (1900)

Let $E$ be an **uncountable** set of real numbers. Is there a bijection

$$f : E \to \mathbb{R}?$$

The Continuum Hypothesis (CH) asserts that Hilbert's 1st problem has a positive solution: if $E$ is uncountable then a bijection $f : E \to \mathbb{R}$ exists.

So is CH true or false. . . ?!

# Dramatis personæ

al-Khwārizmī
c. 780 – c. 850

Tartaglia
1499 – 1557

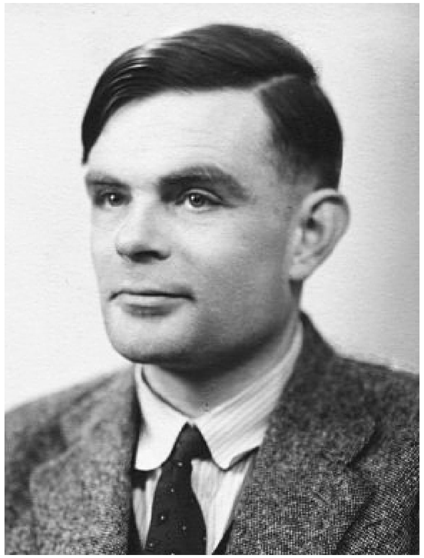
Cardano
1501 – 1576

# Dramatis personæ

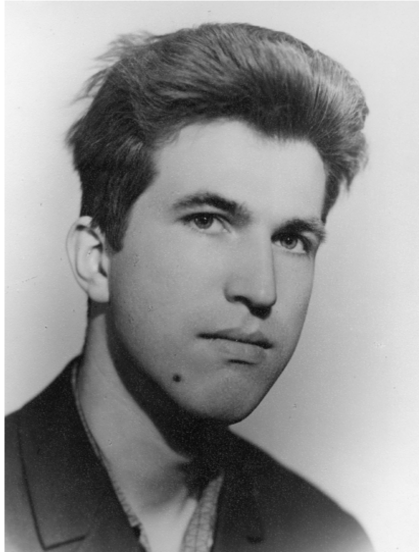
Abel
1802 – 1829

Galois
1811 – 1832

# Dramatis personæ



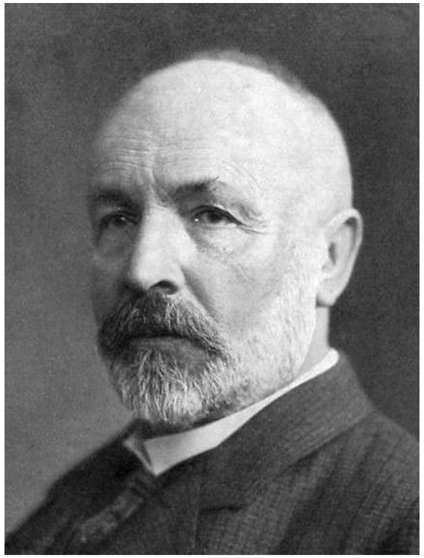
Turing
1912 – 1954



Matiyasevich
1947 –

Wiles
1953 –

# Dramatis personæ

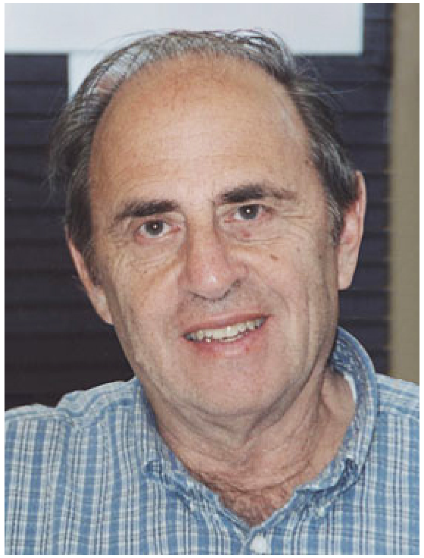


Cantor
1845 – 1918

Hilbert
1862 – 1943

# Dramatis personæ

Gödel
1906 – 1978



Cohen
1934 – 2007