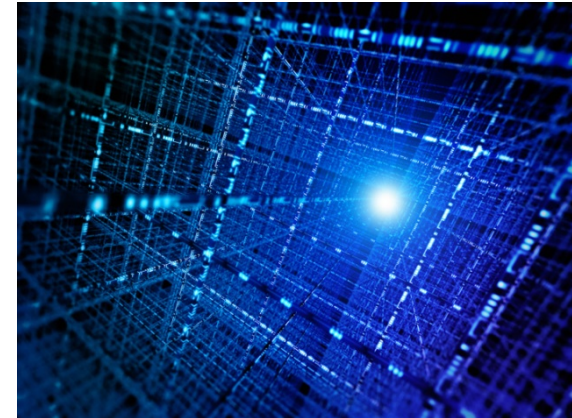
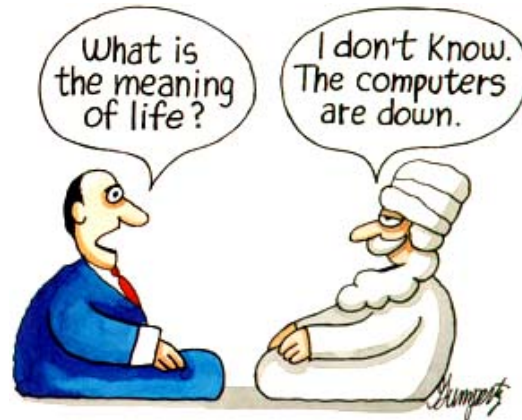
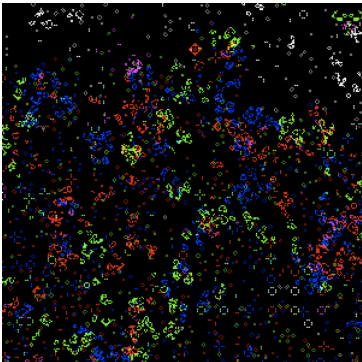


Limits of Computation

Antonina Kolokolova

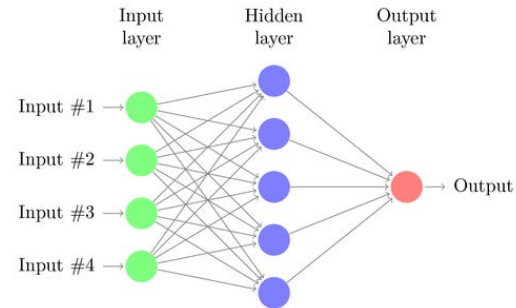


- What is computation?



- What is information?

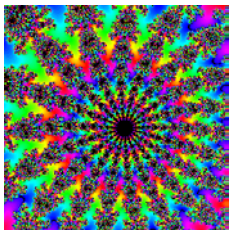
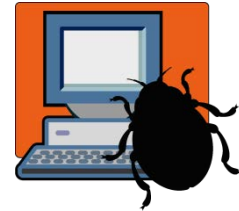
- What is learning?



- Are there any limits of our ability to solve problems?

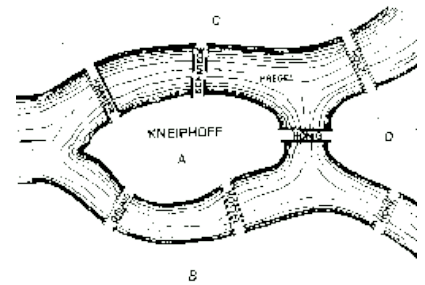
Theoretical Computer Science

- Is there a perfect antivirus?



- Can computers be creative?

- Why some problems are easier than others?



- Is it possible to have secure information and communication?



The science of information

- In many languages the word for “Computer Science” is derived from the word for information

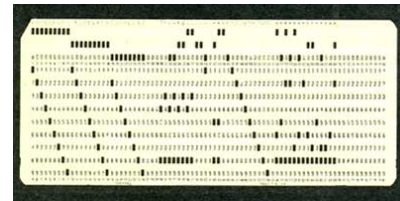
- French: Informatique
- German: Informatik
- Russian: Информатика



- The information comes in and we process it.
- So do computers. So do living cells, etc, etc.

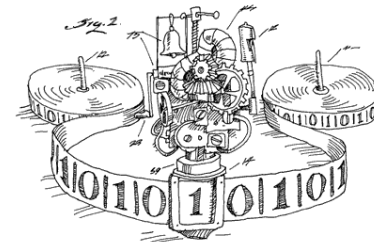
On the other side of iron curtain

- In Soviet Union, in particular in Ukraine, PCs were not around till 1990th
- First photo: “MIR” computer (from 1969). Developed in Kiev by Glushkov and his group.
- Were still in use in 1980s.
- Programmable calculators for personal use

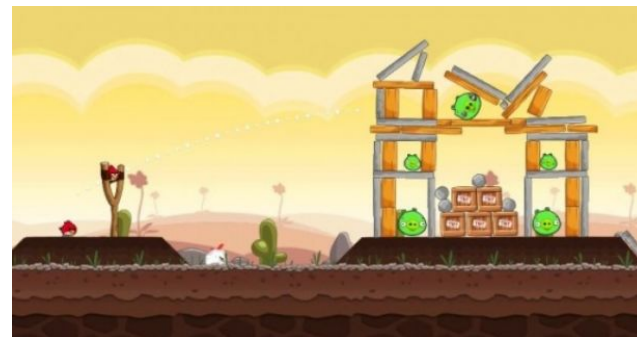




What is computation?



- We process information by doing a “computation on it”. Changing it from one representation to another.



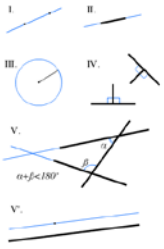
- But what is computation?

– What does your smartphone compute when you are playing Angry Birds?

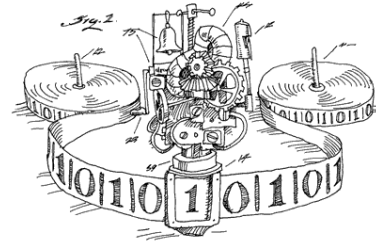
– How does DNA “compute”?



- Is there a limit to what can be computed?



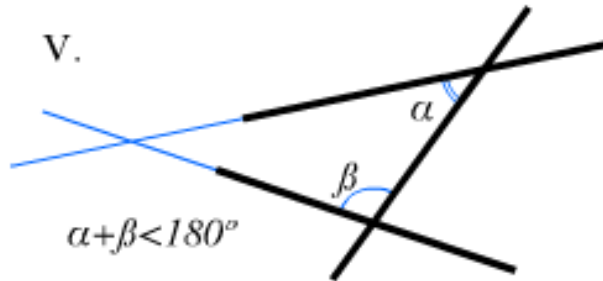
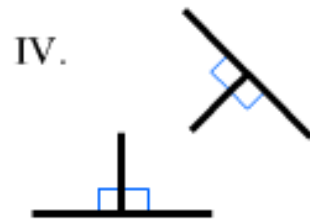
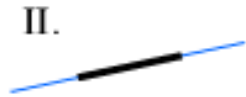
Limits of computation



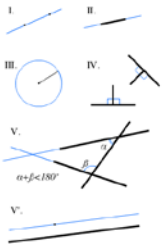
- In 1900, at the International Congress of Mathematicians in Paris, David Hilbert posed a list of 23 problems. Problem 2 asked to prove that mathematics contains no self-contradictions.
- In 1920, Hilbert extended it to what is now known as “Hilbert’s program”



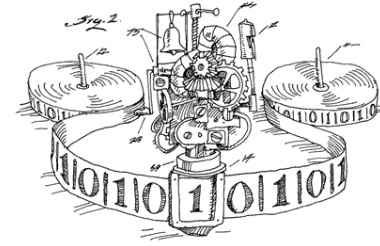
Axioms example: Euclid's postulates



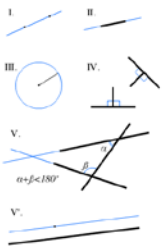
- I. Through 2 points a line segment can be drawn
- II. A line segment can be extended to a straight line indefinitely
- III. Given a line segment, a circle can be drawn with it as a radius and one endpoint as a centre
- IV. All right angles are congruent
- V. Parallel postulate



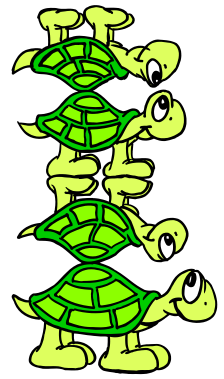
Hilbert's program



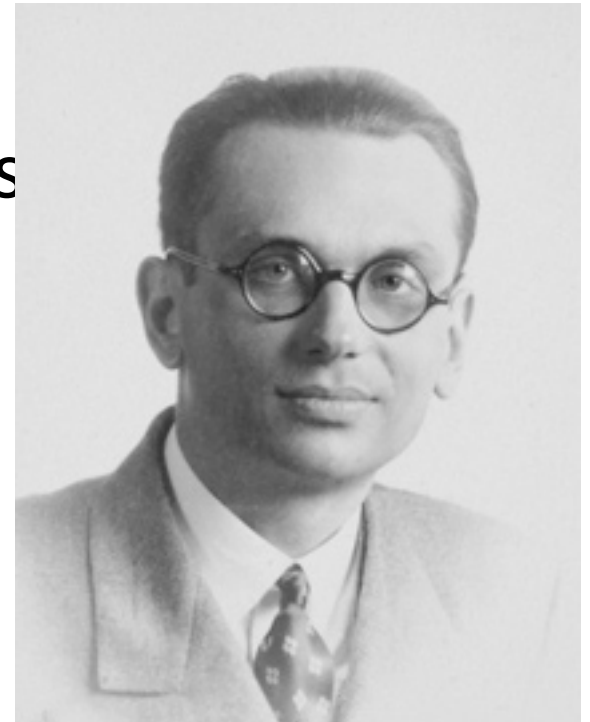
- Express all mathematics in a precise way
- Allowing a formal proof of all true statements
- With a proof, inside mathematics, that there is no self-contradiction
- And a procedure (an algorithm) for deciding, for any given mathematical statement, whether it is true or false.



Gödel Incompleteness Theorem

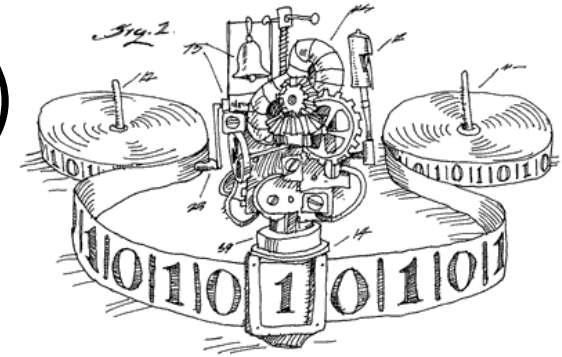


- If mathematics is not self-contradictory...
- Then there are true statements that can't be proven!
- Such as “I am not provable”
- Self-reference leads to something strange, a paradox!



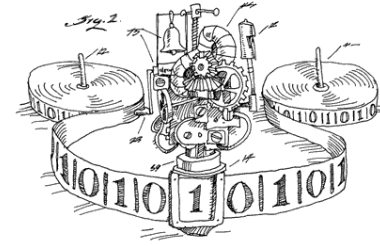
Turing machine

- A Turing machine has an (unlimited) memory, visualized as a tape
- Or a stack of paper
- And takes very simple instructions:
 - Read a symbol
 - Write a symbol
 - Move one step left or right on the tape
 - Change internal state.

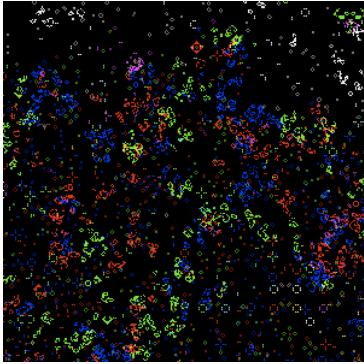


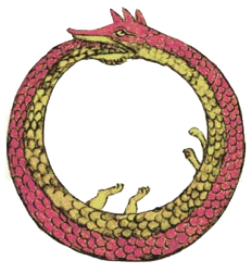


Church-Turing thesis

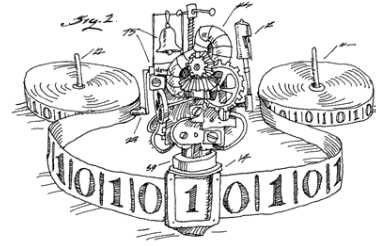


Everything we can call “computable” is computable by a Turing machine.

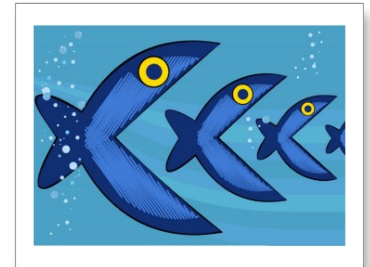




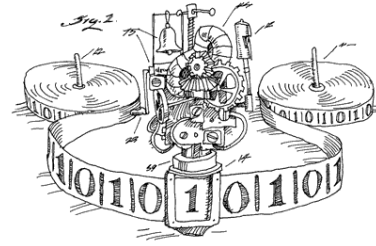
“Will this ever stop?”



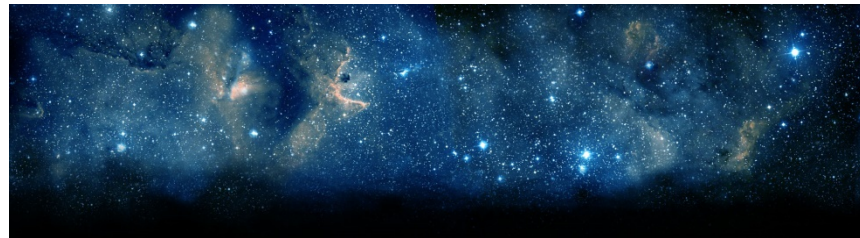
- A code for a Turing machine program is a string.
- Any string can be an input to a program.
- Imagine there is a machine that always does the opposite...
 - From the machine which code is its input
 - On a string encoding it
- What will it do on its own code?
 - Yes?... No?... Yes?... No?... Paradox!
- So no such machine can exist... Some problems are unsolvable, with self-reference to blame.



Complexity of computation

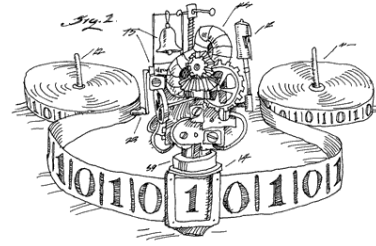



- Would you still consider a problem really solvable if it takes very long time?
 - Say 10^n steps on an n -symbol string?
 - At a billion (10^9) steps per second (~ 1 GHz)?
 - To process a string of length 100...
 - will take $10^{100}/10^9$ seconds, or $\sim 3 \times 10^{72}$ centuries.



- Age of the universe: about 1.38×10^{10} years.
- Atoms in the observable universe: 10^{78} - 10^{82} .

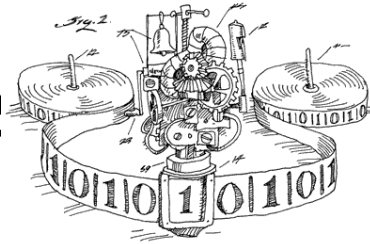
Efficient computation



- What can be computed in our universe?
 - We could only work with very short strings...
 - But we want to work with our DNA string! 
 - We can try being efficient in solving problems.
 - What does it mean to be efficient?
 - And what kinds of problems can be solved efficiently?

A million-dollar question!

Polynomial-time computable



- Efficiently solvable:
 - On an input string of length n
 - Produce a solution roughly in time at most
 - n , or n^2 , or n^3 , or... n^{const} .
 - So a DNA string can be processed in about 3.2×10^9 steps. At 1GHz, it is 3.2 seconds.
- Concept dates back to 1960s, Jack Edmonds, and also Alan Cobham.
 - Edmonds arguing why his “blossom algorithm” is better than what was known before.



Colouring maps

- How many colours needed so that neighbouring countries do not get the same colour?
- For a picture like that – no more than 4.
- (A theorem famous for being proven with a help of a computer)
- Can it be done with 3?



Colouring maps

- Can it be done with 3 colours?
- How do we find out?
 - Look at neighbours of Austria. There are 7 of them... 3 colours not enough.
- In general, nobody knows a good way!



Question

- Can this map be coloured with three colours?



Question

- Can this map be coloured with three colours?



Question

- Can this map be coloured with two colours?



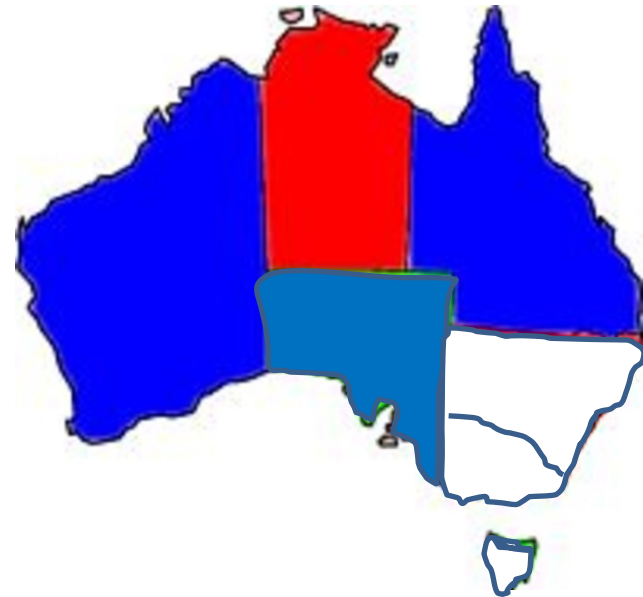
Question

- Can this map be coloured with two colours?
- No...
- Western Australia, Northern territory and South Australia should all be different colours.



Colouring with 2 colours

- How do you check if a map is colourable with 2 colours?
 - Start anywhere.
 - Colour a region red
 - Colour its neighbours blue
 - Colour their neighbours red again...
 - Continue until either done, or found a region would border one of the same colour



Colouring maps

- If somebody gives you a coloured map, easy to check.
 - Check that there are 3 colours overall
 - Check that each country is different from its neighbours.
 - Done!
- Finding a colouring seems much harder...



NP: “guess and check”

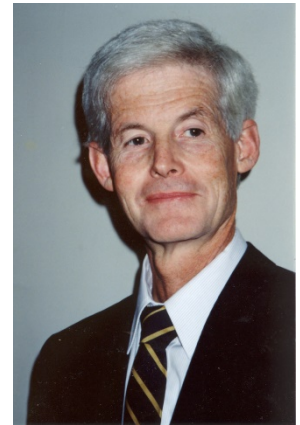
- A lot of problems of the form “guess and check” can be disguised as colouring.
- Or, more generally, constrain satisfaction.
- Many more equivalent problems:
 - Travelling salesperson problem (TSP),
 - Knapsack
 - Scheduling





NP-completeness

- A lot of problems of the form “guess and check” can be disguised as colouring.
- Or, more generally, constraint satisfaction.
- When stated in the form “is there a solution that satisfies the conditions..” these problems are called **NP-complete**.
 - And they are as hard as anything for which there is a guess-and-check algorithm!
- The concept invented by Stephen Cook (and independently Leonid Levin) in 1971
- Made its way into popular culture, often as a synonym to “hard” ... though we do not know for sure!



Stephen Cook



Leonid Levin

P vs. NP

- Find a way to solve any of those efficiently, or show it cannot be done...
 - known as P vs. NP problem

A million-dollar question!

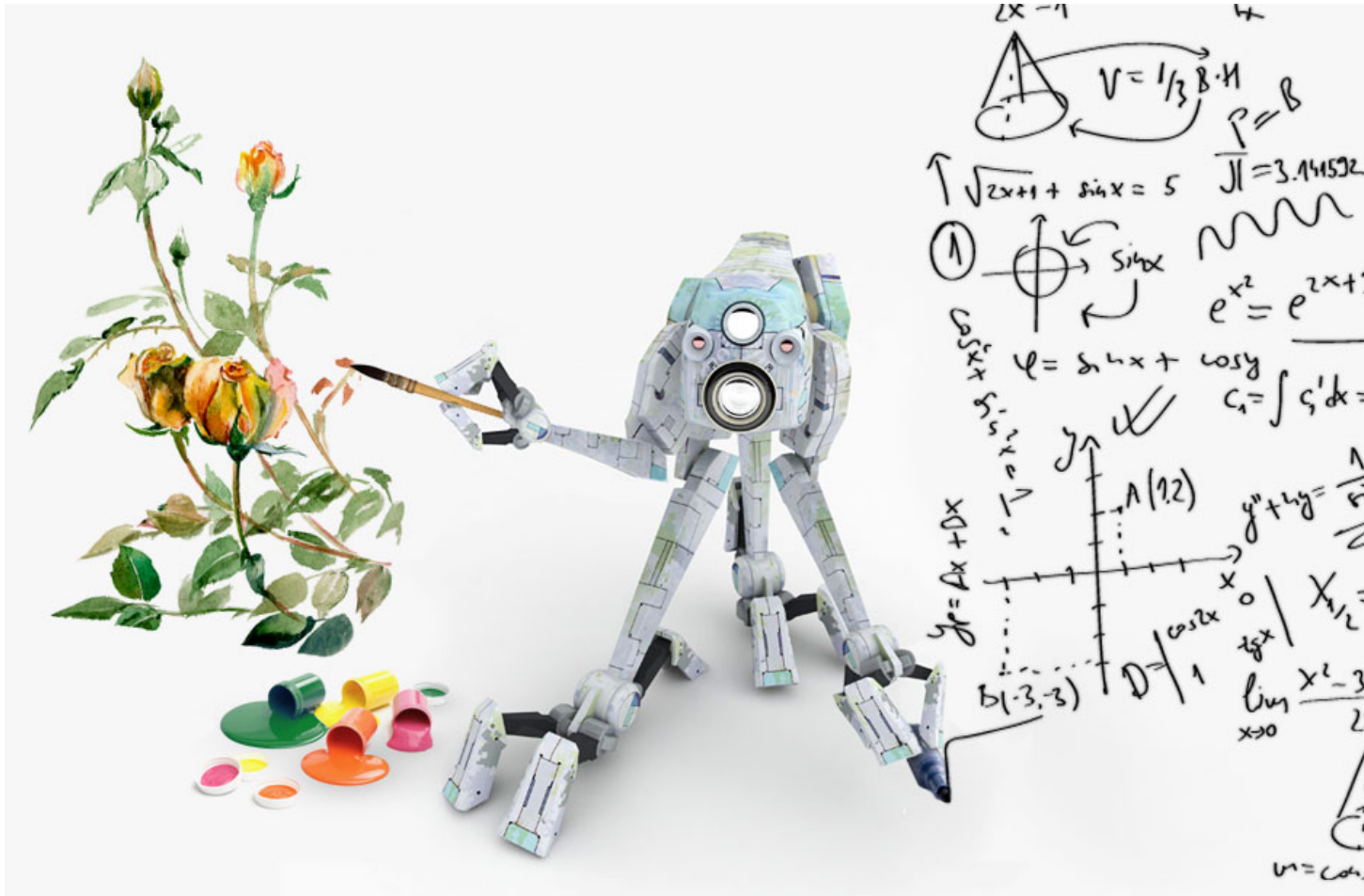


P vs. NP

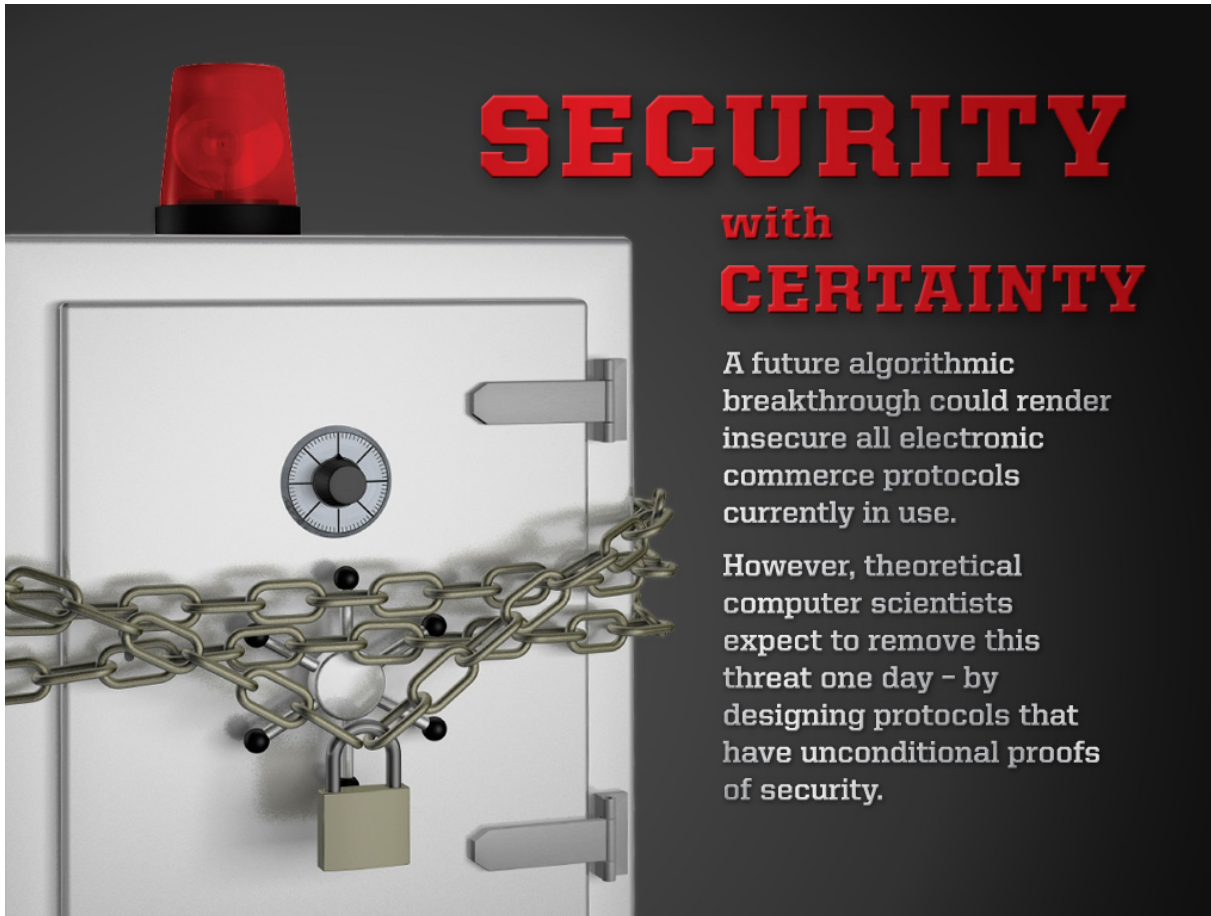
- If somebody finds a way to solve 3-colouring efficiently, then we will live in a very different world, where
 - Creativity and problem-solving are automated.
 - Not much security left on the internet.
 - Every theorem has a short proof...
- So most scientists believe that solving 3-coloring is impossible, but nobody so far can prove it.



If P=NP... creativity is automated



If $P=NP$... there is no security



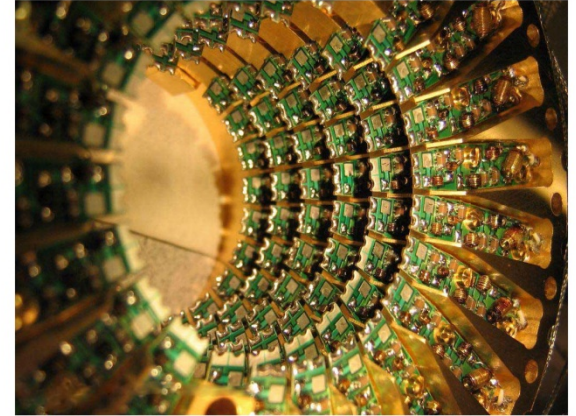
SECURITY
with
CERTAINTY

A future algorithmic breakthrough could render insecure all electronic commerce protocols currently in use.

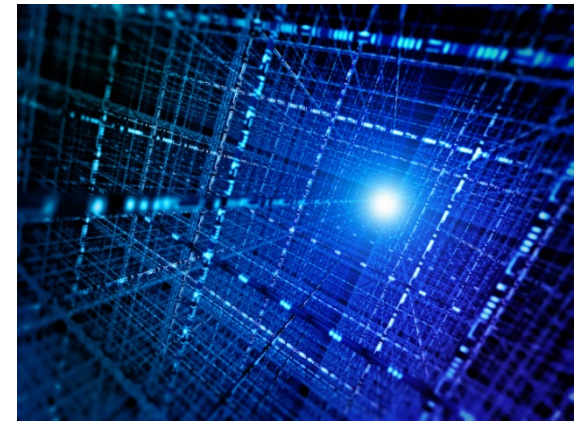
However, theoretical computer scientists expect to remove this threat one day - by designing protocols that have unconditional proofs of security.

Quantum computers

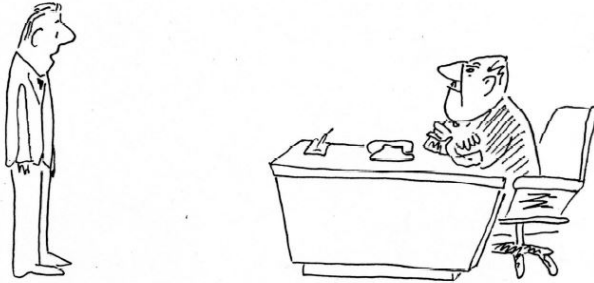
- Can quantum computers colour maps efficiently?
- We don't know... but don't think so.
- Although they can factor numbers, which we do not know how to do on a usual computer fast.
- A real scalable quantum computer would require changing much of security on the internet.
 - RSA cryptosystem assumes factoring is hard.



Adiabatic Quantum Computer Component Array



P vs. NP (David Johnson's cartoons)



"I CAN'T SOLVE IT - I GUESS I'M JUST TOO DUMB."



"I CAN'T SOLVE IT - BECAUSE NO SOLUTION EXISTS!"



"I CAN'T SOLVE IT - BUT NEITHER CAN ALL THESE FAMOUS PEOPLE!"



WE MAY NOT BE ABLE TO SOLVE IT...
BUT WE SURE CAN GET CLOSE!