Background: computation

• Computation is closely related to mathematics.

• Mathematicians have been trying to find informal “algorithms” for centuries, from ancient Greece.

• Euclidean algorithm: Given two positive integers $(a, b)$, find their largest common divisor.

\[
\begin{align*}
q_1 &= \left\lfloor \frac{a}{b} \right\rfloor & a &= b \cdot q_1 + r_1 & r_1 &= a - b \cdot q_1 \\
q_2 &= \left\lfloor \frac{b}{r_1} \right\rfloor & b &= q_2 \cdot r_1 + r_2 & r_2 &= b - q_2 \cdot r_1 \\
q_3 &= \left\lfloor \frac{r_1}{r_2} \right\rfloor & r_1 &= q_3 \cdot r_2 + r_3 & r_3 &= r_1 - q_3 \cdot r_2 \\
q_4 &= \left\lfloor \frac{r_2}{r_3} \right\rfloor & r_2 &= q_4 \cdot r_3 + r_4 & r_4 &= r_2 - q_4 \cdot r_3 \\
q_n &= \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor & r_{n-2} &= q_n \cdot r_{n-1} + r_n & r_n &= r_{n-2} \\
q_{n+1} &= \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor & r_{n-1} &= q_{n+1} \cdot r_n + 0 & r_n &= r_{n-1} / q_{n+1}
\end{align*}
\]
Sieve of Eratosthenes

- Find all prime numbers up to a given number.

- Iteratively remove the multiples of each prime, starting with the first prime number 2.

\[
\begin{array}{cccccccccccccccc}
2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\
2 & 3 & \times & 5 & \times & 7 & \times & 9 & \times & 11 & \times & 13 & \times & 15 & \times & 17 & \times \\
2 & 3 & \times & 5 & \times & 7 & \times & \times & \times & 11 & \times & 13 & \times & \times & \times & 17 & \times \\
\end{array}
\]

Many variants and improvements by Euler, Sundaram, Atkin…
Success and failure

- Ancient Greeks: geometric constructions using only a straightedge without markings and a compass

- Bisect any angle ✓

- Construct an equilateral triangle ✓

- Trisect any angle?

- Doubling of a cube?

- Square the circle?
Geometric constructions using only straightedge and compass

• Solved in 19th century after revolution in abstract algebra.

• Bisect any angle ✓

• Construct an equilateral triangle ✓

• Trisect any angle ∙

• Doubling of a cube ∙

• Square the circle ∙
Geometric constructions using only straightedge and compass

• Any such construction can be viewed as computing a number $c$ has the property

$$[Q(c) : Q] = 2^k$$

The minimum degree of a polynomial over $Q$ that has $c$ as a root is a power of 2.

Line: linear equation

Circle: quadratic equation
Geometric constructions using only straightedge and compass

• Bisect any angle : \( \cos(2x) = 2 \cos^2 x - 1 \).

• Construct an equilateral triangle : height = \( \frac{\sqrt{3}}{2} \).

• Trisect any angle \( \times \) : \( \cos(3x) = 4 \cos^3 x - 3 \cos x \).

• Doubling of a cube \( \times \) : the edge length becomes \( \sqrt[3]{2} \).

• Square the circle \( \times \): the edge length becomes \( \sqrt{\pi} \) which is transcendental over \( \mathbb{Q} \) (not a root of any polynomial with finite degree).
Success and failure

• The previous questions can be viewed as a limited form of computation:
  
• Computing using only straightedge (linear equation) and compass (quadratic equation).

• The more limited the computation, the easier to prove impossibility results.

• Let us see a more general form of computation.
Success and failure

• Finding explicit formulas for the roots of one variable equations.
• Linear equations: \( ax+b=c \) where \( a \) is not 0, \( x=(c-b)/a \).
• Quadratic equations: \( ax^2+bx+c=0 \) where \( a \) is not 0.

\[
x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}
\]

• Cubic equations, formula found by Ferro and Tartaglia in the 16th century.
• Quartic equations, formula found by Ferrari and Cardano in the 16th century.
• Can this go on for larger degrees, e.g., degree 5 equations?
Explicit formulas for roots

• Major open problem from the 16th century, not solved until the 19th century.

• Surprisingly, the answer is NO in general!

• The permutation group $S_5$ is not solvable in general.

• Abel-Ruffini impossibility theorem (1824), Galois theory (1846) further provides a characterization of polynomial equations solvable by explicit formulas.

• Hermite’ 1873: $e$ is transcendental; Lindemann’ 1882: $\pi$ is transcendental (over Q).
Success and failure

• The previous questions can be viewed as a limited form of computation:

• Computing using only finite degree equations, and finding the roots using only arithmetic operations and radicals.

• Let us see a more general form of computation.
Success and failure

• Hilbert’s 10th problem (posed at ICM 1900)

• Given a Diophantine Equation (a polynomial equation with integer coefficients and a finite number of variables), find a process to decide if it has an integer solution.

\[3x^2 - 2xy - y^2z - 7 = 0: x=1, y=2, z=-2\]

What Hilbert is actually asking: an algorithm to solve this problem.
Success and failure

• Hilbert’s 10th problem

• Has such an algorithm been found?

• No! MRDP theorem (1970): no such algorithm exists!

• In modern terminology: Hilbert’s 10th problem is undecidable.
Modern use of computation

Computing the orbits of astronomical objects

Total solar eclipse 8/21/2017

Super blood moon 1/20/2019

Can predict accurately to minutes or seconds
Modern use of computation

Weather forecast

Can predict pretty accurately for the following week
Modern use of computation

GPS routing

Can quickly pick the best route and estimate arrival time
Modern use of computation

Computer graphics in video games

Can create super natural and cool video effects
Modern use of computation

Artificial Intelligence

Can beat human in certain situations
The topic of this course

What is the general theory of computation behind all these applications?
Specific goals

• Computational models.

• Abstract and mathematical models of computation.

• By abstraction we can study the common powers and limitations of ALL computation.
Specific goals

• Computability.

• What can be computed and what cannot be computed?

• The true limits of computers/computation.
Specific goals

- Complexity theory.

- For problems that can be computed, what is the amount of resources (e.g., time, space etc.) needed?

- A more refined and complete understanding of computation.
Specific goals

• Complexity classes.

• A complexity class is a set of problems that can be solved given a certain amount of resources.

• We will see several different complexity classes in this class.

• A major question: the relations between different complexity classes.
P vs NP Problem: one of the 7 (now 6) unsolved millennium problems which can earn you $1M.

If you give a positive answer to this one, you can “solve” all the others! So you get $6M.
We will see some of the classes in this picture.
• What this class is about: concepts, models, proofs…

• What this class is not about: programming and coding….
Textbooks

Required

Computational Complexity
A Modern Approach
Sanjeev Arora
and Boaz Barak

Recommended

Introduction to the Theory of Computation
Third Edition
Michael Sipser