Background: computation

• Computation is closely related to mathematics.

• Mathematicians have been trying to use informal “algorithms” for centuries.

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

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

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

*Many variants and improvements by Euler, Sundaram, Atkin…*
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: $ax^3+bx^2+cx+d=0$ where $a$ is not 0, formula found by Ferro and Tartaglia in the 16th century.
• Quartic equations: $ax^4+bx^3+cx^2+dx+e=0$ where $a$ is not 0, formula found by Ferrari and Cardano in the 16th century.
Success and failure

• Can this go on for larger degrees, e.g., degree 5 equations?

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

• Surprisingly, the answer is NO in general!

• Abel-Ruffini impossibility theorem (1824), Galois theory (1846) further provides a characterization of polynomial equations solvable by explicit formulas.
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 many 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 solve this one, you can “solve” all the others! So you get $6M.
We will see some of the classes in this picture.