

DMA: Induction

Laura Mančinska
(delivered by Jurij Volčič)

Institut for Matematiske Fag

UNIVERSITY OF COPENHAGEN



Corona guidelines



Welcome back to classes and auditorium lectures!
We must follow the following guidelines:



- Don't attend if you have symptoms of COVID-19 – including mild symptoms
- Cough/sneeze into your sleeve



- Keep a minimum distance of one metre
- Avoid using lifts. If you have to use a lift, keep a distance of two metres



- Disinfect your hands when you enter the building
- Disinfect your hands when you enter the classroom/auditorium
- Ensure good hand hygiene – wash and sanitise thoroughly and often



- Upon entering a room; sit to avoid close passage of others
- Pay attention to where you are allowed to sit/not to sit



- Sit at least one metre apart
- Avoid walking around during classes/lectures



- Help clean seats after classes/lectures, and remember to clean spray bottles after use
- Don't share equipment with others



- Empty the room near the exit first
- Leave to room in a calmly manner
- Maintain distance to each other



UNIVERSITY OF COPENHAGEN
FACULTY OF SCIENCE

Plan for this class

- Induction as a proof technique
- Examples

**Reading: Notes on Absalon (can also take a look
Section 2.4 from KBR)**

Suppose we want to prove a mathematical statement or formula

How do we show that

$$1 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Try different values of n :

$$n = 1 \qquad 1 \stackrel{?}{=} \frac{1(1+1)(2 \cdot 1 + 1)}{6} \quad \checkmark \square$$

$$n = 2 \qquad 1 + 2^2 \stackrel{?}{=} \frac{2(2+1)(2 \cdot 2 + 1)}{6} = \frac{2 \cdot 3 \cdot 5}{6} \quad \checkmark \square$$

$$n = 3 \qquad 1 + 2^2 + 3^2 \stackrel{?}{=} \frac{3(3+1)(2 \cdot 3 + 1)}{6} = \frac{3 \cdot 4 \cdot 7}{6} = 14$$

$\checkmark \square$

$$n = 4 \qquad 1 + 2^2 + 3^2 + 4^2 \stackrel{?}{=} \frac{4(4+1)(2 \cdot 4 + 1)}{6} = \frac{4 \cdot 5 \cdot 9}{6} = 30$$

$\checkmark \square$

Is it enough to check for only some values of n ?

- Fermat conjectured that all numbers of the form

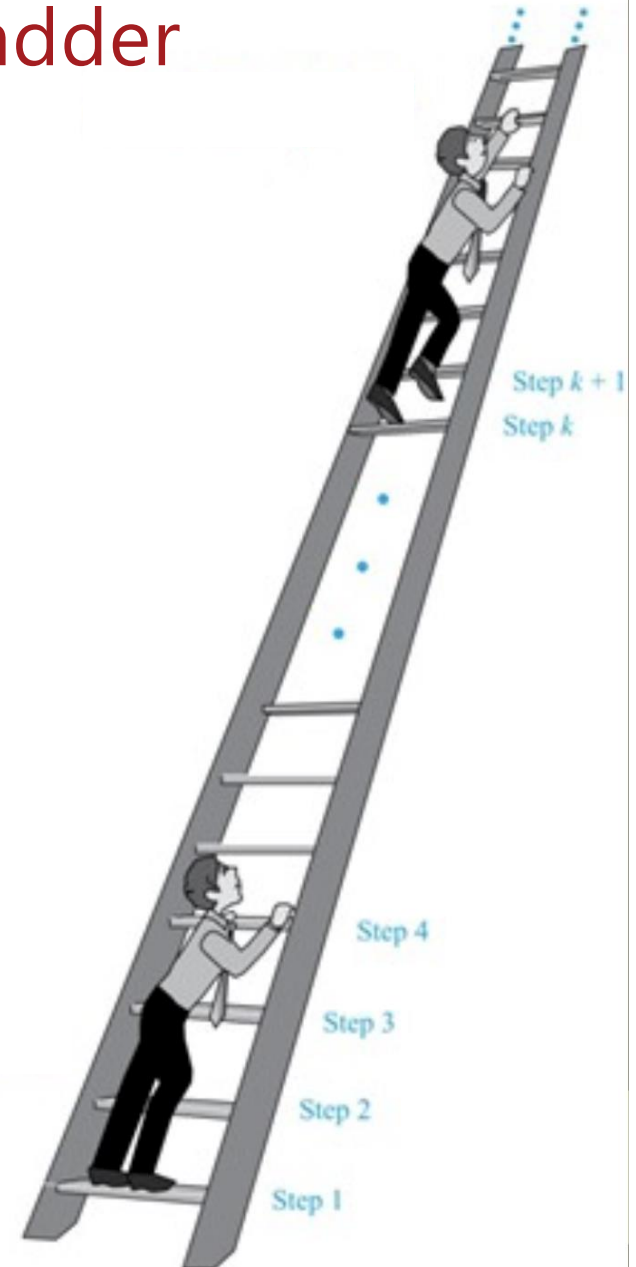
$$F_n = 2^{2^n} + 1 \text{ are prime.}$$

- $F_1 = 2^{2^1} + 1 = 5$
- $F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$
- $F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$
- Fermat checked up to $n = 4$
- 100 years later, Euler noticed that
$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417$$
- There are **no known** Fermat primes F_n with $n > 4$ (checked up to $n = 32$)

Mathematical induction

Analogy: climbing an infinite ladder

- Suppose you can reach the first rung
- If you are on a particular rung k you can get on the next rung $k + 1$



The principle of mathematical induction

Let $P(n)$ be a predicate (statement) defined for integers $\{n_0, n_0 + 1, \dots\}$. If

a) $P(n_0)$ is true and

b) for any $n \geq n_0$, we have that $P(n)$ being true implies that $P(n + 1)$ is true

then

- $P(n)$ is true for all integers $n \geq n_0$.

Terminology

a) Is called **basis step** or base case

b) Is called **induction step**.

Using induction to prove that

$$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6} \text{ for all } n \in \mathbb{Z}^+$$

- Predicate $P(n)$: $\sum_{i=1}^n i^2 = \frac{n(n+1)(2n+1)}{6}$ for $n \geq 1$

- Base case: Check that $P(1)$ holds.

$$\frac{1(1+1)(2 \cdot 1 + 1)}{6} = \frac{1(2)(3)}{6} = 1 = 1^2$$

- Induction step:

Assume that $P(n)$ holds for some $n \geq 1$ (Induction hypothesis)

Show that this implies that $P(n+1)$ holds.

Structure of an inductive proof

- (State that the proof uses induction.)
- Define an appropriate predicate $P(n)$. Identify n_0 .
- Prove that $P(n_0)$ is true.
- Prove that $P(n)$ implies $P(n + 1)$.
- Invoke the principle of mathematical induction.

Example: divisibility statement

Task: Show that $5 \mid (6^n - 5n + 4)$ for any $n \in \mathbb{Z}^+$

Let $b_n = 6^n - 5n + 4$ where $n \in \mathbb{Z}^+$.

Let $P(n)$ be the statement that b_n is divisible by 5.

- **Base case:** Check that $P(1)$ holds.

$$b_1 = 6 - 5 + 4 = 5 \text{ is divisible by 5.}$$

- **Induction step:**

Assume that $P(n)$ holds for some $n \geq 1$ (Induction hypothesis)

We want to show that $P(n + 1)$ holds.

Invariants

An invariant is a property that is preserved throughout a program or a procedure

- $xy = z$ after every iteration of a **for**-loop.
- Temperature of a nuclear reactor doesn't exceed a critical value.

Invariants: Loop invariant (in the Euclidean algorithm)

GCD (X, Y)

```
1  While ( $X \neq Y$ )  
2      If ( $X > Y$ ) then  
3           $X \leftarrow X - Y$   
4      Else  
5           $Y \leftarrow Y - X$   
6  return  $X$ 
```

Let X_n and Y_n be the values of X and Y after n passes.

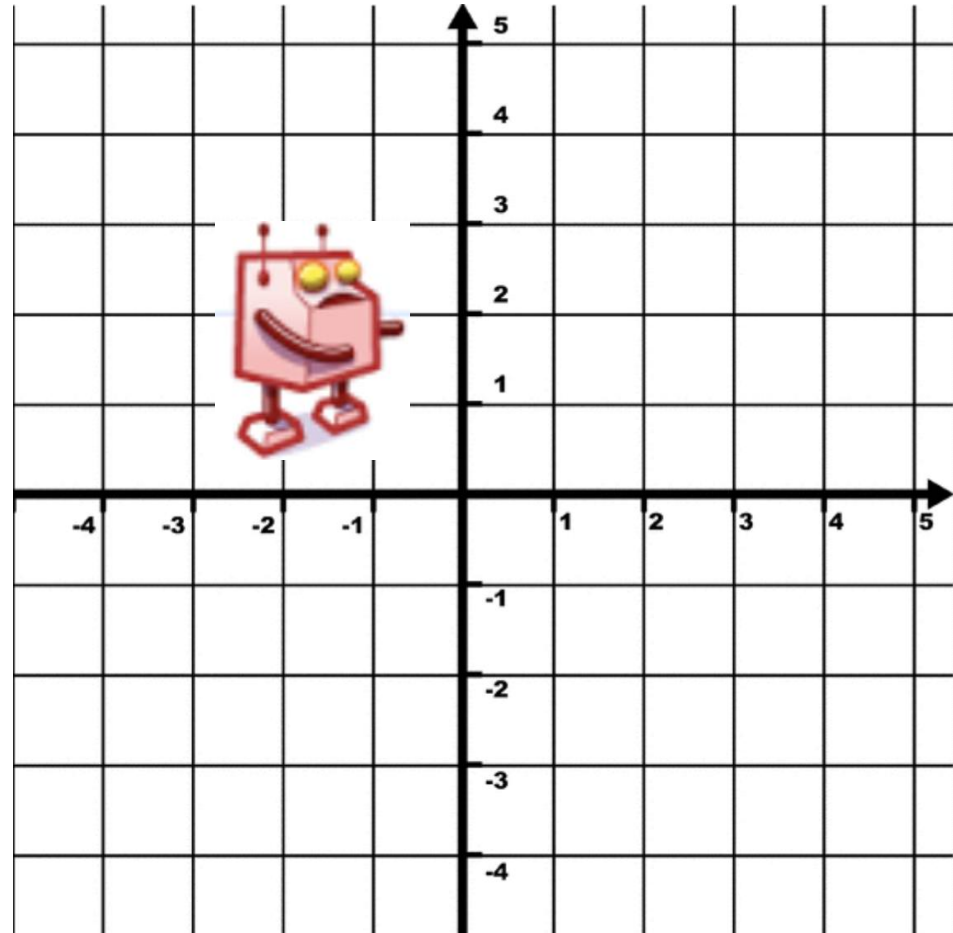
Then $\text{GCD}(X_n, Y_n) = \text{GCD}(X, Y)$

Invariants: Diagonally moving robot on a plane

Robot starts at $(0,0)$

If the robot is at (x, y) after step k , then in step $k + 1$ it can go to either

- $(x + 1, y + 1)$ or
- $(x + 1, y - 1)$ or
- $(x - 1, y + 1)$ or
- $(x - 1, y - 1)$



Can the robot be at $(1,0)$ after some number of steps?

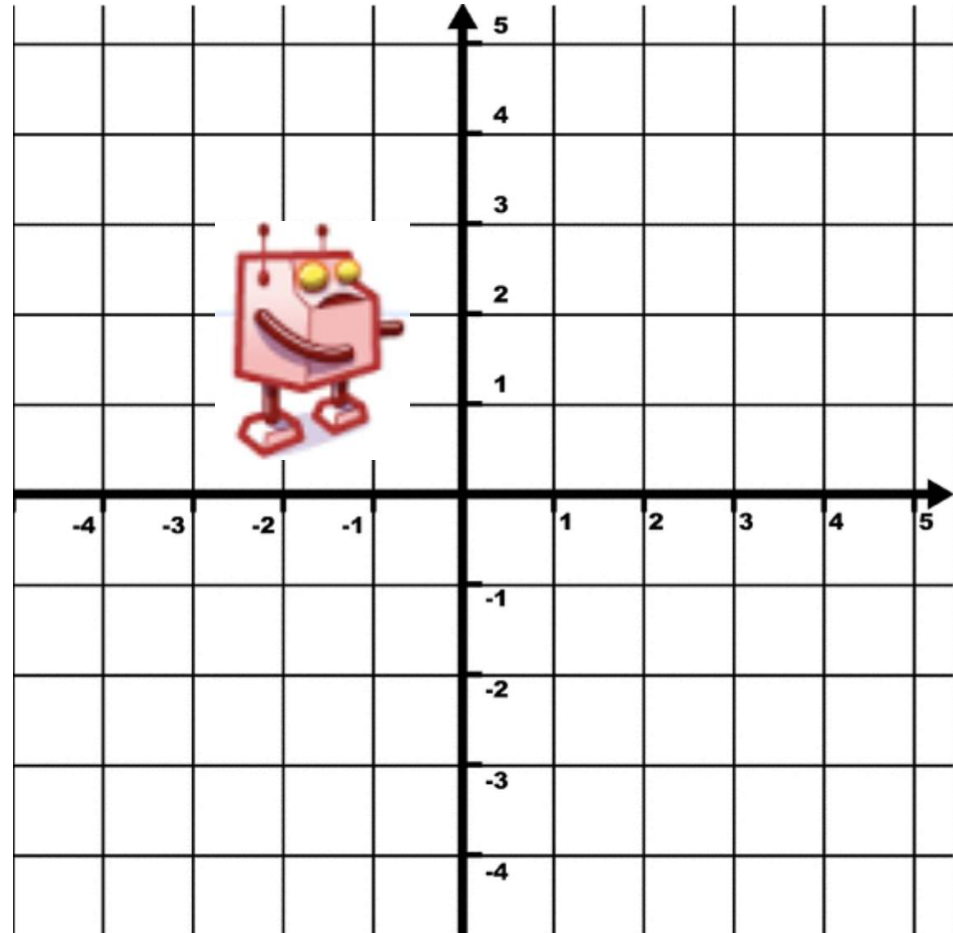
Invariants: Diagonally moving robot on a plane

Robot starts at $(0,0)$

If the robot is at (x, y) after step k , then in step $k + 1$ it can go to either

- $(x + 1, y + 1)$ or
- $(x + 1, y - 1)$ or
- $(x - 1, y + 1)$ or
- $(x - 1, y - 1)$

Can the robot reach $(1,0)$?



Claim. After any number of steps $n \geq 0$ robot's position (x, y) is such that $x + y$ is even.