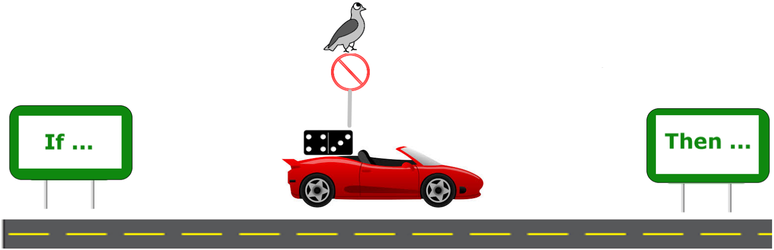
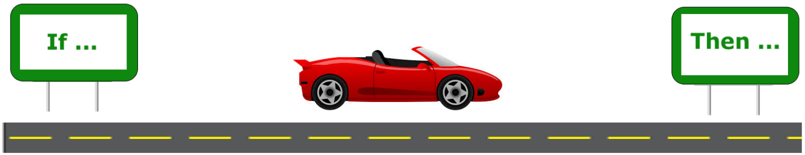
Proof Methods



Myrto Manolaki
myrto.manolaki@ucd.ie

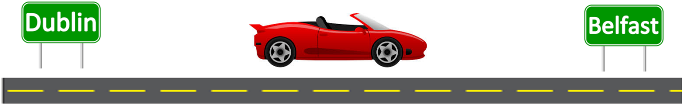
February 2, 2019

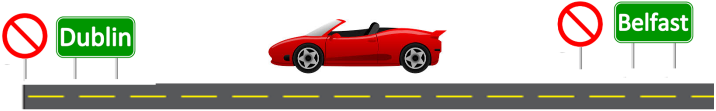


Mathematical statements consist of an **assumption** (usually followed by "if") and a **conclusion** (usually followed by "then"). Our objective is to **start with the assumption** and after a number of logical steps **reach the conclusion**. A **proof** is a logical path connecting the assumption with the conclusion. There are many proof methods, but we shall focus on the following:

1. Proof by Contradiction.
2. Separating Cases.
3. Mathematical Induction/Strong Mathematical Induction.
4. Pigeonhole Principe/General Pigeonhole Principle.

Proof by Contradiction





Suppose that we want to show that
"**If D is true, then B is true**". It suffices to show that
if B is NOT true, then D cannot be true.

Example

(1) Let m be a positive integer. If m^2 is even show that m is even.

Proof.

For the sake of contradiction we **assume that the conclusion is not true**, i.e. that m is not even. This means that $m = 2k + 1$ for some integer k. We want to show that m^2 cannot be even! We have:

$$m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1,$$

which means that m^2 is odd. This **contradicts** our assumption that m^2 is even. Thus the conclusion is true, i.e. m is even. □

Exercise

(2) Let m be a positive integer. If m^2 is odd show that m is odd.

♣ A number r is called **rational** if it can be expressed as a quotient $\frac{m}{n}$ of two integers m and n (with $n \neq 0$). If r doesn't have such an expression, is called **irrational**. For example, 0.25 is rational because $0.25 = \frac{1}{4}$.

Example

(3) Show that $\sqrt{2}$ is irrational.

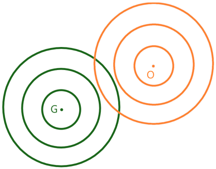
Proof.

Assume that $\sqrt{2}$ was rational. Then $\sqrt{2} = \frac{m}{n}$ for some integers m and n (with $n \neq 0$). We can also assume that m and n do not have any common *prime factors* (if they had, we would eliminate them). By squaring: $2 = (\sqrt{2})^2 = \left(\frac{m}{n}\right)^2 = \frac{m^2}{n^2} \Leftrightarrow m^2 = 2n^2$.
Thus m^2 is even and so m is even by Ex. (1), which means that $m = 2k$ for some integer k.
Replacing we get: $4k^2 = (2k)^2 = 2n^2 \Leftrightarrow n^2 = 2k^2$. Thus n^2 is even and so n is even by Ex. (1). This is a contradiction because m and n have 2 as a common factor. Thus $\sqrt{2}$ is irrational. $\square$

Exercise (4) Suppose that we paint the entire plane with green and orange colour so that every point is either orange or green and **both** colours exist in our painting). Show that for each positive number d there exist two points with different colour whose distance is exactly d.

Proof.

For the sake of contradiction we assume that **there exists** a positive number d such that **for each** two points which have distance d, their colour has to be the same. Thus, if G is a green point, then the circles centred at G with radii d, $2d$, $3d$, ... have to be green. By choosing an orange point O, we see that the corresponding orange circles will intersect the green circles, which yields a **contradiction** (since each point has one colour).



□

♣ It is important to know that when we take the negation of a statement:

- "**for all**" (denoted by $\forall$) becomes "**exists**" (denoted by $\exists$)
- "**exists**" becomes "**for all**"
- "**or**" becomes "**and**"
- "**and**" becomes "**or**"

(* Here "or" is not exclusive, meaning that the cases it connects can occur simultaneously.)
For example, the **negation** of the sentence
"I have a brother **or** a sister" (i.e. "I have siblings") is
" I do **not** have a brother **and** I do **not** have a sister".

Separating Cases

♣ There is a natural way to extend the notion of powers to (positive) irrational numbers, preserving all the good properties we have for powers involving integers.

Exercise (5) Show there are two irrational numbers a and b such that a^b is rational.

Hint: Consider the number $(\sqrt{2})^{\sqrt{2}}$ and separate two cases:

1. $(\sqrt{2})^{\sqrt{2}}$ is rational.
2. $(\sqrt{2})^{\sqrt{2}}$ is irrational.

For **case 1**: take $a = \sqrt{2}$ and $b = \sqrt{2}$. Then a^b is rational.
For **case 2**: take $a = (\sqrt{2})^{\sqrt{2}}$ and $b = \sqrt{2}$. Then $a^b = (\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\sqrt{2}} = (\sqrt{2})^2 = 2$ which rational!

Be careful: When you separate cases make sure you covered each possible scenario! (A real number will be either rational or irrational-there is no other option. But it is wrong to say that a real number will be either even or odd!)

Mathematical Induction

Mathematical induction is a very useful tool in Mathematics. The general idea is that when we want to prove a statement for ALL natural numbers it suffices to do the following steps:

1. Prove the statement for the first number.
2. If we **assume** that the statement is correct for a natural number k, then we should prove that the statement is correct for the next number $k + 1$.

Example

(6) What formula we would get if we sum the first n odd numbers?

To guess the correct formula we calculate and try to find a pattern:

$$\begin{aligned} 1 &= 1 = 1^2 \\ 1+3 &= 4 = 2^2 \\ 1+3+5 &= 9 = 3^2 \\ 1+3+5+7 &= 16 = 4^2. \end{aligned}$$

So, suppose we have n terms in our sum, these terms being the first n positive odd numbers. The nth term is in fact $2n-1$ and the sum is

$$1+3+5+\cdots+2n-1.$$

Following the pattern above, we believe that this sum should equal n^2, so that the formula

$$1+3+5+\cdots+(2n-1) = n^2$$

should be true.

However, we have not proved this yet. To prove statements for natural numbers (like the one just discussed) we should apply the **method of mathematical induction**. In this method we should follow 3 steps:

- We check that the statement is true for the **first** number. (Here we have checked that the formula is true for $n = 1$, 2, 3, 4.)
- We assume that the statement is true for some particular value of k. We call this our **induction hypothesis**.
- We then try to prove the statement for the next number succeeding k, namely $k + 1$, using the induction hypothesis. We call this the **induction step**.

In our example, when try to make the induction step, we are required to prove that

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = (k + 1)^2.$$

Here, we have added the $(k + 1)$th odd number, which is $2k + 1$, to the previous sum to form the sum to $k + 1$ terms.
But now, by the induction hypothesis,

$$1 + 3 + 5 + \cdots + 2k - 1 = k^2.$$

We add $2k + 1$ to each side of this equation and obtain

$$1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1) = k^2 + 2k + 1.$$

But $k^2 + 2k + 1 = (k+1)^2$, and hence

$$1 + 3 + 5 + \cdots + (2k-1) + (2k+1) = (k+1)^2.$$

This completes the induction step, and proves that the formula holds for all values of n.

To sum up: Suppose that we have a statement $P(n)$ involving the natural number n. In our example, the statement $P(n)$ was the equality

$$1 + 3 + 5 + \cdots + 2n - 1 = n^2.$$

- Suppose that $P(1)$ is true.
- Suppose also that for any particular number k, the truth of $P(k)$ implies the truth of $P(k+1)$.

Then $P(n)$ is true for all positive integers n.

Example

(7) Let $x \geq -1$ be a real number. Then the inequality

$$(1+x)^n \geq 1+nx$$

is true for all positive integers n.

We will prove this inequality by mathematical induction.
Let $P(n)$ be the proposition that $(1+x)^n \geq 1+nx$.

- $P(1)$ is the statement that

  $$(1+x)^1 \geq 1+1\cdot x.$$

  Since $(1+x)^1 = 1+x$, we conclude that $P(1)$ is true.
- We assume that $P(k)$ is true. Thus we assume that

  $$(1+x)^k \geq 1+kx.$$

- We want to prove that $P(k+1)$ is true.

Example Continued

$P(k+1)$ is the statement that

$$(1+x)^{k+1} \geq 1 + (k+1)x.$$

Now since we are assuming that $x \geq -1$, it follows that $1 + x \geq 0$. Then we may multiply each side of the inequality $(1+x)^k \geq 1 + kx$ by $1 + x$ and obtain

$$(1+x)(1+x)^k \geq (1+x)(1+kx).$$

This gives

$$(1+x)^{k+1} \geq 1 + kx + x + kx^2 = 1 + (k+1)x + kx^2.$$

Example Continued

But $kx^2 \geq 0$ for any real number x, as x^2 is a square, and hence

$$1 + (k+1)x + kx^2 \geq 1 + (k+1)x.$$

Thus we have

$$(1+x)^{k+1} \geq 1 + (k+1)x + kx^2 \geq 1 + (k+1)x.$$

This implies that $P(k+1)$ is true and completes the induction step. Thus $P(n)$ is true for each positive integer n.
♣ We call the inequality described by $P(n)$ *Bernoulli's Inequality*.

Example

(8) Examine for which positive integers n, the inequality

$$2^n \geq n^2$$

is true.
Let $P(n)$ be the proposition that $2^n \geq n^2$.
We can see that $P(1)$ and $P(2)$ are true, but $P(3)$ is false, because

$$2^3 = 8 < 3^2 = 9.$$

But $P(4)$ is true, as $2^4 = 16 = 4^2$.

Example Continued

We propose to prove that $P(n)$ is true if $n \geq 4$, and we do this by mathematical induction.
We assume that $P(k)$ is true, where $k \geq 4$.
This means that $2^k \geq k^2$ is true.
Now we want to prove that $P(k+1)$ is true. This means that

$$2^{k+1} \geq (k+1)^2 \text{ is true.}$$

Since $2^k \geq k^2$ is true we may multiply by 2 to obtain

$$2 \times 2^k = 2^{k+1} \geq 2k^2.$$

Now we simply need to prove that $2k^2 \geq (k+1)^2$ if $k \geq 4$.

Example Continued

Consider the number

$$2k^2 - (k+1)^2.$$

This equals

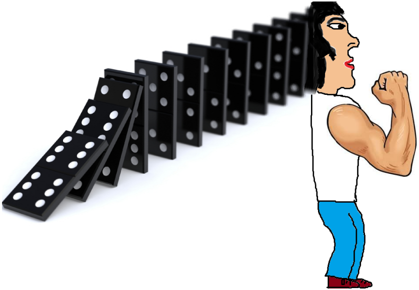
$$2k^2 - (k^2 + 2k + 1) = k^2 - 2k - 1 = (k-1)^2 - 2,$$

which is positive if $k \geq 4$. Hence $P(k+1)$ is true if $k \geq 4$. Thus it is true that $2^n \geq n^2$ if $n \geq 4$.

Remark: As we saw in the above example, in mathematical induction **we do not necessarily have to start by** $n = 1$. This means that if we want to prove a statement for all integers $n \geq n_0$, where n_0 is a fixed integer, it suffices to do the following steps:

- Show that $P(n_0)$ is true.
- Assume that $P(k)$ is true for some $k \geq n_0$ and use this to show that $P(k+1)$ is true.

Strong Mathematical Induction



Sometimes the normal mathematical induction is not enough to prove what we want. We have a stronger kind of mathematical induction, which is called strong mathematical induction and has the following steps:

- We show that $P(1)$ is true.
- We assume that $P(1), P(2), \ldots, P(k)$ are true and we use this information to show that $P(k+1)$ is true.

Then the statement $P(n)$ is true for all positive integers n.

Example

(9) Which positive integers can be written as a sum of 3's and 5's? For example we have:

$3 = 3 \qquad 5 = 5 \qquad 6 = 3 + 3$
$8 = 3 + 5 \qquad 9 = 3 + 3 + 3 \qquad 10 = 5 + 5$
$11 = 3 + 3 + 5 \qquad 12 = 3 + 3 + 3 + 3$

We will show that all integers $n \geq 8$ can be written as a sum of 3's and 5's.

Solution:

Statement $P(n)$: the integer n can be written as a sum of 3's and 5's.

- We checked that $P(8)$ is true. (Also we saw that $P(9), P(10), P(11), P(12)$ are true.)
- We suppose that for $k \geq 8$ we have that $P(8), P(9), \ldots, P(k)$ are true. We will use this to show that $P(k+1)$ is true.

Example Continued

The (strong) inductive hypothesis tells us that for $k \geq 8$ we have that each of the numbers $8, 9, \ldots, k$ can be written as a sum of 3's and 5's.

We observe that: **k+1=(k-2)+3**.

Case 1: If $8 \leq k - 2 \leq k$. Then by using our inductive hypothesis we have that $k - 2$ is a sum of 3's and 5's. Hence $k + 1 = (k - 2) + 3$ is also a sum of 3's and 5's. This means that $P(k + 1)$ is true for Case 1.

Case 2: If $k - 2 < 8$. This implies $k = 8$ or $k = 9$ (because also k is an integer greater or equal to 8). But we have already seen that $P(9) = P(8 + 1)$ and $P(10) = P(9 + 1)$ are true. This means that $P(k + 1)$ is true for Case 2.

Conclusion: $P(k + 1)$ is true for each case. Hence by strong mathematical induction we have that $P(n)$ is true for all integers $n \geq 8$, which completes the proof.

In the above example we needed strong induction because we had to jump 2 (and not 1) steps backwards to use the inductive hypothesis. An other important application of strong mathematical induction is the "Fundamental Theorem of Arithmetic". To formulate this we need the following definition:

⧫ An integer number $n \geq 2$ is called a prime if the **only** positive integer numbers a and b which satisfy the equation $n = ab$ are the numbers 1 and n.

For example $2, 3, 5, 7, 11, 13, 17, 19$ are primes, but 21 and 25 are not primes (because $21 = 3 \times 7$ and $25 = 5 \times 5$).

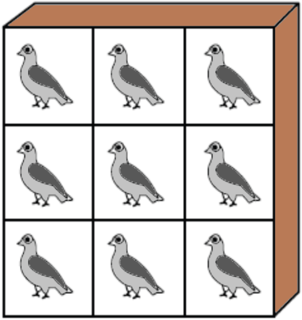
The Fundamental Theorem of Arithmetic

Each integer $n \geq 2$ is either a prime or it can be written as a product of primes.

(The proof, which is omitted, uses strong mathematical induction.)

The Pigeonhole Principle

"If we must put $N + 1$ (or more) pigeons into N pigeonholes, then some pigeonhole must contain at least 2 pigeons."



(General Pigeonhole Principle) "If we must put $Nk + 1$ (or more) pigeons into N pigeonholes, then some pigeonhole must contain at least $k + 1$ pigeons."

Exercises

(10) 100 students are seated (equidistant) at a round table and more than half are boys. Show that there are (at least) 2 boys who are seated diametrically opposite each other.

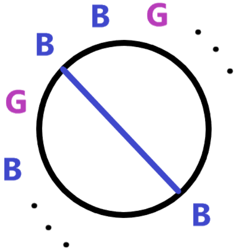
(11) Show that in this room there are at least 2 people with the same number of friends within the room. (Unlike real life, we assume that if A considers that B is his friend, then also B considers A as his friend.)

(12) 51 points are scattered inside a square with a side of 100cm. Prove that some set of 3 of these points can be covered by a square of side 20 cm.

Exercise (10)

Proof.

We will apply the **Pigeonhole Principle**. The pigeonholes are the diameters, which are 50. The pigeons are the boys, which are more than 50. Thus, some diameter (pigeonhole) must contain at least 2 boys (pigeons).



□

Exercise (11)

Proof.

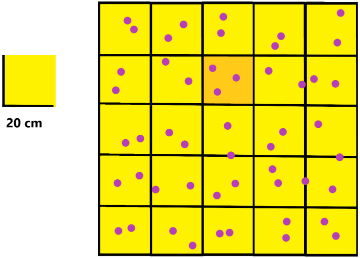
Suppose that there are N people and let a_n be the number of friends of the nth person, where $n = 1, 2, \ldots, N$. Everyone is friend with himself, hence a_n is an integer between 1 and N.

- **Case 1:** If for some $i = 1, 2, \ldots, N$ we have $a_i = N$.
  This means that there is a very popular person who is friend with everyone else. Thus, for each $n = 1, 2, \ldots, N$, the number a_n is an integer between 2 and N (since even the least popular person would have (at least) 2 friends: himself and the popular ith person). The pigeonholes are the $N - 1$ distinct numbers $2, 3, \ldots, N$ and the pigeons are the N numbers $a_1, a_2, \ldots, a_N$.
- **Case 2:** If for every $n = 1, 2, \ldots, N$ we have $a_n < N$.
  The pigeonholes are the $N - 1$ distinct numbers $1, 2, \ldots, N - 1$ and the pigeons are the N numbers $a_1, a_2, \ldots, a_N$.

In both cases, the **Pigeonhole Principle** implies that at least 2 of the N numbers $a_1, a_2, \ldots, a_N$ must be the same integer. □

Exercise (12)

Proof.



We split the given square into 25 squares of side 20cm (as in the picture)*. The conclusion follows by the **General Pigeonhole Principle**, where the pigeonholes are the 25 squares and the pigeons are the $51 = 2 \cdot 25 + 1$ points (i.e. $N = 25$ and $k = 2$).

***Detail:** We have to make sure that each point belongs to exactly one small square. Thus we assume that all squares include the sides at south and west but not the ones at north and east (except the squares touching the the northern/eastern boarder of the large square, where we include the corresponding sides). □