G30 MATH SEMINAR
1 - PROOFS BY CONTRADICTION

1. Introduction

In mathematics, we are interested in *objects* (*e.g.* integers, real numbers, sets, vector spaces, functions, ...) and by *statements* about these objects. To describe an object, we need a *definition*, which has, in mathematics, to be unambiguous (for example, the sentence "a number is called *small* if it is close to 0" is not a definition, as it is not possible with this definition to determine if 0.5 is small).

A (mathematical) statement is a sentence or a sequence of mathematical symbols which has a well defined and unambiguous meaning. It can be true or false. For example:

- "$4 = 2 + 2$" is a statement (which is true);
- "$5 = 2 + 7$" is a statement (which is false);
- "9 is not a prime number" is a statement (which is true);
- "$3 + 4$" is not a statement;
- "$4 + 5 = 9+$" is not a statement;
- "0.5 is small" is not a statement (except if "small" is well defined).

The main aim of mathematicians is to prove *theorems*. A theorem is a statement which has been proved to be true. A *proof* of a statement is a sequence of sentences with logical connections which ensure logically the truth of the statement. If such a proof exist, we say that the statement is proved and it becomes a theorem. Here is an example of a theorem and its (correct) proof:

Theorem 1.1. *For three integers a, b and c, if a divides b and b divides c then a divides c.*

Proof. By definition, a divides b means that there exists an integer k such that $b = ka$. In the same way, b divides c means that there exists an integer ℓ such that $c = \ell b$. We deduce that $c = \ell b = \ell k a$. As the product of two integers is an integer, ℓk is an integer. Therefore, by definition, a divides c. □

Note that sentences like "it is obvious" or "everybody knows that" are not proofs of this theorem.

Usually, we distinguish in a theorem

(i) The hypotheses: these are the conditions which are supposed to be true (for example, in Theorem 1.1, it is "a, b and c are integers" and "a divides b and b divides c");
(ii) the conclusion: in Theorem 1.1, "a divides c".

Finally, note that the fact that, for some reason, we are not able to find a proof does not necessarily imply that the statement is false. For example:

Theorem 1.2. *If n is an integer greater or equal to 3, then the equation*

$$x^n + y^n = z^n$$

admits no (strictly) positive integer solution.

(this theorem, known as *Fermat's Last Theorem* has been proved by Andrew Wiles in 1994).

2. Proofs by contradiction - the method

The example we saw in previous section is called a *direct proof*. We will see a useful tool when direct proofs do not work. The idea of a proof by contradiction is the following one. If we want to prove that a statement is true, we suppose that its hypotheses are true and its conclusion is false. Then, we prove something which contradict either an hypothesis, either some definition. But, as no hypothesis or definition can be false, it implies that the conclusion is in fact true. Here is the example presented in this session:

Theorem 2.1. *There is no rational number (that is a number which can be written as a quotient of two integer) the square of which is 2.*

Proof. Suppose *for the sake of contradiction* that there is a rational number $r \in \mathbb{Q}$ such that $r^2 = 2$ (1). By definition of a rational number, there exist two integers $a \in \mathbb{Z}$ and $b \in \mathbb{N}_{>0}$ such that $r = a/b$. If we consider all pairs of integers (a, b) with $b > 0$ such that $a/b = r$, there is one such that b is minimal. We fix this choice.

Now, as $2 = r^2 = a^2/b^2$, we get $2b^2 = a^2$. Therefore, 2 divides a^2. As 2 is a prime number, by Euclid's Lemma, 2 divides one of a or a so 2 divides a. By definition, it means that there is an integer a' such that $a = 2a'$. We deduce that $2b^2 = 4a'^2$ and therefore $b^2 = 2a'^2$. Using once again Euclid's Lemma, 2 divides b and there is a (positive) integer b' such that $b = 2b'$. From that, we concludes that $r = a/b = a'/b'$. As $b' < 2b' = b$, it contradicts the fact that b is minimal such that $r = a/b$ (2). Finally, there is no rational number the square of which is 2. □

Note that the sentence (2) says that we proved something contradictory. So something before has to be false. On the other hand, the only thing that we can not be sure of in this proof is the sentence (1). Therefore, the statement (1) is false.

Recall that an positive integer n is called *prime* if it has exactly two distinct positive divisors (which are necessarily 1 and n: 1 is not prime). Let us see two other examples of proofs by contradiction:

Theorem 2.2. *The only positive number which is not divisible by any prime number is 1.*

Proof. Suppose *for the sake of contradiction* that there is a positive number n, greater than 1, such that n is not divisible by any prime number (1). Let n be the smallest possible such number. As n is not divisible by a prime number, it is not prime itself. As, moreover, it is divisible by at least two positive integer, 1 and itself, it has at least a third positive divisor m. We have $1 < m < n$ so, as n is the smallest possible number bigger than 1 with no prime divisor, then m has a prime divisor p. Thanks to Theorem 1.1, p

divides n. So it contradicts the fact that n has no prime divisor (2) and any positive number with no prime divisor is 1. □

Theorem 2.3. *There are infinitely many prime numbers.*

Proof. Suppose *for the sake of contradiction* that there are only finitely many prime numbers (1). Then, there is a maximal prime number p. Let us consider the (big) number

$$N = 1 \times 2 \times 3 \times \cdots \times (p-1) \times p + 1.$$

Let us prove that N is not divisible by any prime number. Indeed, any prime number q satisfy $1 \leqslant q \leqslant p$ so it divides $1 \times 2 \times 3 \times \cdots \times (p-1)$. If q was also dividing N (1') then it would divide $N - 1 \times 2 \times 3 \times \cdots \times (p-1) = 1$. But 1 has no prime divisor so it is a contradiction (2'). It finishes to prove that N is not divisible by any prime number. Thanks to Theorem 2.2, $N = 1$. Therefore, $1 \times 2 \times 3 \times \cdots \times (p-1) \times p = 0$. As this is impossible with $p > 0$, it is a contradiction (2). Therefore, there are infinitely many prime numbers. □

Notice that in this proof, we used two contradictions arguments (1-2) and (1'-2').

3. Exercises

Exercise 3.1. Which one of the following sentences are (mathematical) statements?

(i) "$4 \times 5 = 20$";
(ii) "$7/8 = 78$";
(iii) "$(3 \times 4 = 4) + 8$";
(iv) "There are not so many prime numbers smaller than 18";
(v) "There are finitely many prime numbers smaller than 18".

Exercise 3.2. Use a direct proof to prove the following statements:

(i) Let $x, y \in \mathbb{Z}$. If x and y are odd then xy is also odd.
(ii) Let $a, b, c \in \mathbb{Z}$. If a divides b and a divides c then a divides $b + c$.
(iii) Let $a \in \mathbb{Z}$. If a^2 divides a then $a \in \{-1, 0, 1\}$.
(iv) Let $n \in \mathbb{Z}$. Either a^2 is divisible by 4 either $a^2 - 1$ is divisible by 4.

Exercise 3.3. Use a proof by contradiction to prove the following statements:

(i) Let $n \in \mathbb{Z}$. If n^2 is odd then n is odd.
(ii) The number $\sqrt[3]{2}$ is not rational.
(iii) Let $a, b, c \in \mathbb{Z}$. If $a^2 + b^2 = c^2$ then a or b is even. [Hint: use one statement of the previous exercise.]
(iv) Let $n \in \mathbb{N}$. If $\sqrt{n}$ is rational then it is an integer.