SAMPLES OF PROOFS

0.1. **What the proofs are about.** With any *proof* we try to derive a new fact out of the facts which we already know. Mathematical proofs do that with the help of logic described in the two previous sections. It may thus seem that mathematics reduces to formal manipulations with sequences of symbols, and a theorem is simply a statement which is "true" according to a truth table. That, however, is not the case. Mathematicians, with a possible exceptions of logicians never manipulate with meaningless formal sequences of symbols. (In fact, logicians also do not do that; they only discuss what may be a result of such a manipulations.)

Mathematicians operate with plain language, possibly pictures and formulas, in order to explain why a certain interesting and non-obvious statement is true. The best, and maybe historically the first example of a mathematical proof would be Pythagoras theorem. You may recall any (there are quite a few) proof of this fact, and think whether this proof has anything to do with truth tables and logical manipulations. (In fact, it does, but this connection is not what we want to emphasize and even discuss in this class.)

We typically do not care about arbitrary statements: there are too many of them, and the life is too short.

Example The statement *The* 9999999999999999*-th digit after the dot in the decimal expansion of* π *is* 7 may be true or false, and there is no reason to prove or disprove it. The statement *One encounters the digit* 7 *only finitely many times in the decimal expansion of* π also may be true or false, and sounds much more enticing. In both cases, nobody knows the answer. For the first statement, nobody cares although it is relatively easy to find out, while for the second one nobody knows how to prove or disprove the statement, and would be proud to do that. The difference is informal and substantial.

We also do not care to prove "obvious" statements. The word "obvious" here may have different meanings.

Example The statement $3 + 2 = 5$ is so "obvious" that we are not going to prove it (in this class, at least).

Example The statement *A square of an even integer is even while a square of an odd integer is odd* is also "obvious", but this time that means "easy to prove". This statement was partially proved in Example 3.1, and one can easily finish that prove along the same lines (do that!). These proofs above are indeed a bit boring. These facts are obvious, and one needs them for a proof of a non-obvious and beautiful fact that $\sqrt{2}$ is not a rational number (i.e. $\sqrt{2} \notin \mathbb{Q}$). See Proposition 15.2 for the proof (do that now!).

Let us for time being accept the following definition (later on you will find it unacceptably naive).

A real number x is called rational if there exist two integers p and q such that

$$x = \frac{p}{q}.$$

As an exercise in notations introduced so far, convince yourself that this definition is equivalent to

$$\mathbb{Q} = \left\{ x \in \mathbb{R} \mid (\exists p \in \mathbb{Z}) \wedge (\exists q \in \mathbb{Z}) : x = \frac{p}{q} \right\}.$$

The quantity $\sqrt{2}$ provides us with an example of a real number which is not rational:

$$\sqrt{2} \in \mathbb{R} \quad \text{while} \quad \sqrt{2} \notin \mathbb{Q}.$$

We call real numbers which are not rational *irrational*, and $\sqrt{2}$ is a standard example of an irrational number.

The following statements are obvious (i.e. "easy to prove", and I strongly suggest to do that as an exercise!)
The sum, product, difference, and ratio of a rational and an irrational number is irrational.
The sum, product, difference and ratio (with a non-zero denominator) of two rational numbers is rational.

What about if both numbers are irrational? Let us consider products. We have examples:

$$\sqrt{2}\,\sqrt{2} = 2,$$

and

$$\sqrt{2}(1 + \sqrt{2}) = 2 + \sqrt{2}.$$

These examples show that the product of two irrational numbers may be both rational and irrational. As an exercise, consider sums, differences, and ratios. In all cases, you need to either present a proof that you always produce rational (irrational) answer, or give examples which demonstrate that both possibilities may occur.

The situation becomes more involved when we consider powers. In fact, examples are still available, however not that easy to find, and a less straightforward proof may be closer to the point.

Proposition 1. *An irrational number taken to an irrational power may come out as rational.*

Proof. We know that $\sqrt{2}$ is irrational. Consider two numbers

$$x = \sqrt{2}^{\sqrt{2}} \quad \text{and} \quad y = x^{\sqrt{2}}$$

The number x may be either rational or irrational while

$$y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2$$

is rational. Now, if x is rational, than this number is an example desired, while if x is irrational, then y provides us with a desired example. $\square$

Please note that in the above proof we still have not found out (and do not care) whether x was rational. We also cannot conclude which particular quantity, x or y, is an example which we wanted. We simply know for sure that one of them does the job.

EXERCISE. Prove the above proposition in a straightforward way. To do that, show that both numbers

$$\sqrt{10} \quad \text{and} \quad 2\log_{10} 11$$

are irrational.

0.2. **Knight's tour.** Mathematical statements and proofs are not necessarily about numbers. Other objects may be considered. Let us consider a well-known puzzle. A knight's tour is a sequence of moves of a knight on a chessboard such that the knight visits every square only once. You may read some funny history and details at http://en.wikipedia.org/wiki/Knight%27s_tour .
Hunting for the solutions of the puzzle is not a homework in this class (it maybe in your CS class).

Let us modify the puzzle slightly. We call a modified chessboard a usual 8×8 chessboard with two squares, lower left and upper right taken away. Of course our modified chessboard has only 62 squares.

Proposition 2. *There is no knight tour on our modified chessboard.*

Proof. Recall that usually a chessboard has its squares colored in black and white. Note that a knight changes the color of the square with every move. Thus any chessboard which admits a knight's tour may have either equal amounts of black and white squares (if the number of moves in a tour is odd), or the difference between these amounts should be one (if the number of moves in a tour is even). Our modification took away 2 squares of the same color, and the difference between these amounts is now 2. Thus our modified chessboard does not admit knight tours. □

0.3. **Infinitude of the set of primes.** This is a classical example of a "proof by contradiction". The rough scheme of such proofs may be presented as follows. We want to prove a statement, call it p. In order to do that, we prove that

$$(\neg p \Longrightarrow q) \quad \text{and} \quad q \quad \text{is false,}$$

or, if you prefer, we prove

$$(\neg p \Longrightarrow q) \bigwedge (\neg q).$$

Here q is some statement which we are free to choose. It is an easy exercise to check that the the above statement can only be *true* if p is *true*, therefore we may prove it instead of proving p directly. In other words we have that

$$\Big(\neg p \Longrightarrow q) \bigwedge (\neg q) \Big) \Longrightarrow p.$$

It may be more transparent to explain as follows. If p was false then something impossible happens, thus p must hold true. Let us now see how these ideas of proof work.

Recall that a natural number $p > 1$ is prime if it has no factors other than itself and 1. Furthermore, it is easy to prove (try to do that now!) that for every natural number n there exists a prime q which divides n. (In particular, if n is a prime itself, then $q = n$.)

Proposition 3. *There are infinitely many primes.*

Proof. Suppose there are finitely many primes. We list all the primes as $p_1, p_2, ..., p_n$. Set $x = p_1 p_2 \dots p_n + 1$ (the product of all primes plus 1) and observe that no prime from the list is a factor of x. Now let q be a prime which divides x. Then q is a prime not appearing on the list, a contradiction. $\square$