Introduction to Proofs
IAP 2015
Lecture Notes 2 (1/6/2015)

1. Overview

We continue to develop our study of methods of proof by examining several examples of arguments dealing with properties of the integers. We give several examples of proofs of rationality for particular real numbers, and conclude with an introduction to mathematical induction and combinatorial reasoning.

2. Working with integers

2.1. **Using quantifiers to construct familiar collections of integers.** Applying the set constructor notation and the concept of quantifiers discussed in Lecture Notes 1, we may write down formal descriptions of the set of (non-negative) *even integers* as

$$\begin{aligned}\{n \in \mathbb{N} : n \text{ is even}\} &= \{m \in \mathbb{N} : \text{there exists } k \in \mathbb{N} \text{ such that } m = 2k\} \\ &= \{2n : n \in \mathbb{N}\}.\end{aligned}$$

These sets are equal to one another, and membership in either set each may be taken as a definition for what it means for an integer to be even. Similarly, we can define the (non-negative) odd integers as

$$\begin{aligned}\{n \in \mathbb{N} : n \text{ is odd}\} &= \{m \in \mathbb{N} : \text{there exists } k \in \mathbb{N} \text{ such that } m = 2k+1\} \\ &= \{2n+1 : n \in \mathbb{N}\}.\end{aligned}$$

Making further use of the quantifiers "for every" and "there exists", we can define many familiar mathematical objects. The importance of this idea is that once we have written down precise definitions (often in the language of sets), we can reason about these objects using many of the logical tools we described in the previous lecture notes.

As an example, let us write down a definition of the set of prime numbers. For this we will need to introduce a few auxiliary concepts along the way (which will also be useful for the discussion in the following sections):

> We say that a natural number $n \in \mathbb{N}$ is *divisible by* another natural number $r \in \mathbb{N}$ (also written as $r|n$) if there exists $k \in \mathbb{N}$ with $n = rk$.
> The set of *divisors* of a natural number $n \in \mathbb{N}$ is then the set
>
> $$\begin{aligned}D(n) &:= \{r \in \mathbb{N} : r|n\} \\ &= \{r \in \mathbb{N} : \text{there exists } k \in \mathbb{N} \text{ s.t. } n = rk\}.\end{aligned}$$
>
> Here, the symbol ":=" indicates that the term on the left – in this case, $D(n)$ – is *defined by* the expression on the right side. Moreover, the abbreviation "s.t." stands for "such that".
> The set of *prime numbers* is then the set
>
> $$P := \{p \in \mathbb{N} : D(p) = \{1, p\}\}.$$

Exercise 2.1. Show that for any $n \in \mathbb{N}$, the set $D(n)$ has finitely many elements. (*Hint: Can you identify an inequality satisfied by r for all $r \in D(n)$?*)

Exercise 2.2. Show that $P := \{p \in \mathbb{N} : |D(p)| = 2\}$, where $|D(p)|$ denotes the number of elements in the (finite) set $D(p)$.

2.2. **Rational numbers and proofs of irrationality.** Recall that a rational number $q \in \mathbb{Q} \subset \mathbb{R}$ is a real number of the form

$$q = \frac{m}{n}$$

for two integers $m, n \in \mathbb{Z}$, with $n \neq 0$. An *irrational number* is then an element of $\mathbb{R} \setminus \mathbb{Q}$. In this section, we continue to develop our discussion of various methods of proof by examining a variety of proofs of irrationality for certain real numbers.

Example 2.3. There is no rational number $x \in \mathbb{Q}$ such that $x^2 = 2$.

Proof. Suppose for contradiction that we could find $m, n \in \mathbb{Z}$ with $n \neq 0$ and

$$\left(\frac{m}{n}\right)^2 = 2.$$

Choose $m', n' \in \mathbb{Z}$ with $n' \neq 0$ such that

$$\frac{m}{n} = \frac{m'}{n'}$$

and the integers m' and n' share no common factor (for instance, write the prime factorizations

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i}$$

and

$$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_j^{\beta_j}$$

and let d be the product of all factors appearing in both m and n; now, set $m' = m/d$ and $n' = n/d$).

We then have

$$(m')^2 = 2(n')^2, \tag{1}$$

so that $(m')^2$ is divisible by 2. It follows that $m' = 2\ell$ for some $\ell \in \mathbb{Z}$. We therefore have

$$(m')^2 = 4\ell^2. \tag{2}$$

Combining (1) and (2), we obtain $(n')^2 = 2\ell^2$ and therefore conclude that n' is divisible by 2. This contradicts the construction that m' and n' have no common factors. □

Remark 2.4. It follows from the intermediate value theorem of calculus (which we will briefly discuss when we begin to work with arguments involving the set of real numbers) that there exists $x \in \mathbb{R}$ with $f(x) = x^2 - 2 = 0$.

Example 2.5. Show that $e = \sum_{k=0}^{\infty} \frac{1}{k!}$ is irrational.

Proof. Suppose for contradiction that there existed $m, n \in \mathbb{Z}$ with $n \neq 0$ and $e = \frac{m}{n}$. We then have

$$ne = m, \quad \text{and thus} \quad k!ne = k!m$$

for every $k \in \mathbb{N}$. Fix $k \in \mathbb{N}$, to be determined later in the proof. Expanding $k!ne$ using our definition of e gives

$$k!ne = k!n\left(1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{k!}\right) + k!n\left(\frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \cdots\right). \tag{3}$$

The first term on the right-hand size is then an integer, while the second term is bounded from below by $\frac{n}{k+1}$ and from above by $\frac{n}{k}$ (to see this, write

$$\begin{aligned} k!n&\left(\frac{1}{(k+1)!} + \cdots\right) \\ &= n\left(\frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} + \cdots\right) \\ &\leq n\left(\frac{1}{k+1} + \frac{1}{(k+1)^2} + \frac{1}{(k+1)^3} + \cdots\right) \\ &= \frac{n}{k} \end{aligned}$$

where to obtain the last inequality we have used the formula for the sum of a geometric series, $\sum_{k\geq 1} a^k = \frac{a}{1-a}$ for $a \in \{a \in \mathbb{R} : |a| < 1\}$). For k sufficiently large, the second term in (3) is therefore strictly between 0 and 1, so that $k!ne$ not an integer for any such k.

On the other hand, the quantity $k!m$ (which, by assumption, is equal to $k!ne$) is clearly an integer. This gives the desired contradiction. □

Remark 2.6. We have (a bit loosely) used some properties of limits of sequences in the above proof – we postpone discussion of these notions.

Example 2.7. Show that there exist $x, y \in \mathbb{R} \setminus \mathbb{Q}$ with $x^y \in \mathbb{Q}$.

Remark 2.8. Before proceeding, we need to give a meaning to x^y when x and y are possibly irrational. This can be done by setting

$$x^y := \exp(y \log(x))$$

for $x > 0$, $y \in \mathbb{R}$. By standard properties of the exponential and logarithm functions, this definition is consistent with all the familiar algebra rules for exponents (provided that one works in the setting of positive real numbers).

Proof. Recall that by Example 2.3 above, $\sqrt{2}$ is irrational. Consider two cases:

Case 1: $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$. In this case the result is immediate with $x, y = \sqrt{2}$.

Case 2: $\sqrt{2}^{\sqrt{2}} \in \mathbb{R} \setminus \mathbb{Q}$. Take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We then have

$$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$$

which is clearly rational. The result therefore holds in this case as well.

Since the result holds in both cases, the desired claim follows. □