Math 2001 Lecture 15.

06.21.2022.

Last time:

- Proofs by contrapositives or contradictions
- Proving equivalences
- Suggestions for mathematical writing.

Today:

- Existence proofs
  - constructive or nonconstructive
- Second worksheet on proofs

1. Existence proofs

Point: Construction and verification of a valid example is sufficient for proving an existence claim.

Easy examples:

Prop: There exists an even prime number.

Pf: The number 2 is such an example.

Prop: There exists an integer that can be written as a sum of two perfect cubes in two different ways.

Pf: Consider the number 1729. We have

$$1729 = 10^3 + 9^3 = 1^3 + 12^3,$$

one can find such a number w/ some program

So 1729 suffices as an example.

Rmk: The point on the previous page should be contrasted with the following: to prove an object (a kind of object) with a certain property does not exist, it is not sufficient to give only one particular instance of such an object that doesn't have that properties.

Eg. Show that there isn't any real number $x \in \mathbb{R}$ with $x^4 < x < x^2$. (i.e., disprove "$\exists\, x \in \mathbb{R}$ s.t. $\underbrace{x^4 < x < x^2}_{(*)}$")

The number $x = 2$ fails $(*)$, but this failure alone isn't sufficient as a proof of the underlined statement.

to find k, l in general look up "Euclidean algorithm".

A harder existence proof:

Prop: Let $a, b \in \mathbb{Z}_{>0}$. Then $\exists\, k, l \in \mathbb{Z}$ s.t. $\gcd(a,b) = ka + lb$.

E.g. $a = 10,\ b = 12 \Rightarrow \gcd(10, 12) = 2.$ $\quad 2 = (-1)\cdot 10 + 1 \cdot 12$

$a = 3,\ b = 5 \Rightarrow \gcd(3, 5) = 1.$ $\quad 1 = (-3)\cdot 3 + 2 \cdot 5$

Pf: Consider the set $D = \{ xa + yb : x, y \in \mathbb{Z} \}$, and let d be the smallest positive integer in D. We claim that $d = \gcd(a,b)$, so that $d = k\cdot a + l\cdot b$ for some $k, l \in \mathbb{Z}$, as desired, and we'd be done.

To prove the claim that $d = \gcd(a,b)$, we first prove that $d \mid a$ and $d \mid b$. To prove $d \mid a$, let $r \in \{0, 1, \dots, d-1\}$ be the remainder obtained when we divide a by d. So $a = dq + r$ for some $q \in \mathbb{Z}$.

We have $r = a - dq$. But $d \in D$ so $d = xa + yb$ for some $x, y \in \mathbb{Z}$.

So $r = a - dq = a - (xa+yb)q = (1-xq)a + (-yq)b \in D$.

Since $d \in D$, $0 \le r < d$, and d is the smallest positive int in D, it follows that $r = 0$, so $d \mid a$.

A similar argument shows that $d \mid b$.

Now, to show $d = \gcd(a,b)$, we note:

(1) $d \le \gcd(a,b)$ since we just showed that d is a common divisor of a and b.

(2). $\gcd(a,b) \le d$: we have $\gcd(a,b) \mid a$, $\gcd(a,b) \mid b$, so $\gcd(a,b) \mid xa+yb$ $\forall x, y \in \mathbb{Z}$. In particular, $\gcd(a,b) \mid d$ since d is a $\mathbb{Z}$-lin. comb. of a and b.

By (1) and (2), we conclude that $d = \gcd(a,b)$, so we are done. $\square$

Take away from the proof: The gcd. of two positive integers equals the smallest positive integral lin. comb. of the two integers.

$$\gcd(a,b) = \min\left(\{xa+yb \mid x,y\in\mathbb{Z}\} \cap \mathbb{Z}_{>0}\right)$$

Some related problems:

<u>7.31.</u> If $n \in \mathbb{Z}$, then $\gcd(n, n+1) = 1$.

Pf: We can write 1 as a $\mathbb{Z}$-lin. comb of n and $n+1$:

$$1 = 1\cdot(n+1) + (-1)\cdot n,$$

and 1 is the smallest positive int, so it must be the smallest positive lin comb. of $n+1$ and n, so it must be the gcd of n and $n+1$, i.e., $\gcd(n, n+1) = 1$. $\square$

7.32. If $n \in \mathbb{Z}$, then $\gcd(n, n+2) \in \{1, 2\}$.

Pf: Let $n \in \mathbb{Z}$. We note that $2 = 1 \cdot (n+2) + (-1) \cdot n$, ie., the number 2 is a pos. $\mathbb{Z}$-lin. comb. of $n+2$ and n, so

$$\gcd(n, n+2) \leq 2.$$

It follows that $\gcd(n, n+2) \in \{1, 2\}$. $\square$

(An alternative proof: It suffices to show that if d is any common divisor of n and $n+2$, then $d \leq 2$. Suppose d is such a common divisor, then since $d \mid n+2$ and $d \mid n$ we have $d \mid (n+2) - n = 2$, so $d \leq 2$, as desired. $\square$)

2. Constructive vs. non-constructive proofs

Recall: $(x^a)^b = x^{(ab)}$

We'll prove the following prop. in two ways.

Prop: There exist irrational numbers x, y s.t. x^y is rational.

Pf 1: (constructive) Take $x = \sqrt{2}$ and $y = \log_2 9$. We know that x is irrational, and we have

$$x^y = \sqrt{2}^{\log_2 9} = \sqrt{2}^{\log_2 (3^2)} = \sqrt{2}^{2\log_2 3} = (\sqrt{2}^2)^{\log_2 3} = 2^{\log_2 3} = 3 \in \mathbb{Q},$$

so it remains to check that y is irrational.

We prove $y \notin \mathbb{Q}$ by contradiction: suppose otherwise, ie, suppose $y \in \mathbb{Q}$, then $\log_2 9 = \frac{m}{n}$ for some $m, n \in \mathbb{Z}_{>0}$. Thus, we have

$2^{m/n} = q$, so $q^n = (2^{m/n})^n = 2^m$. This is impossible since q^n is odd while 2^m is even, so y must be irrational, and we are done. $\square$

Pf 2: (non-constructive) Consider $x = \sqrt{2}$, $y = \sqrt{2}$, so that $x^y = \sqrt{2}^{\sqrt{2}}$ and $x, y \notin \mathbb{Q}$.

If $\sqrt{2}^{\sqrt{2}} = x^y \in \mathbb{Q}$, then we are done.

If $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, then we may take $x' = \sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ and $y' = \sqrt{2} \notin \mathbb{Q}$ and we'd have $(x')^{y'} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$, so again we are done. $\square$