Math 2001. Lecture 23.

03.11.2022.

Last time:
- There are infinitely many primes.
- Worksheet 2 on proofs.

Today: Ch 7: Beyond conditional proofs.

1. Equivalences

(a): "if and only if" statements ($P \Leftrightarrow Q$)

Typical proof strategy:

prove the two implications separately.

E.g. Let $x \in \mathbb{Z}$. Prove that x is even iff $3x+5$ is odd.

Pf: (1) ($\Leftarrow$) We first prove that x is even if $3x+5$ is odd, by proving the contrapositive. So suppose x is not even. Then x is odd, therefore $x = 2k+1$ for some $k \in \mathbb{Z}$. It follows that $3x+5 = 3(2k+1)+5 = 6k+8 = 2\underline{(3k+4)}$, so $3x+5$ is even. It follows that x is even if $3x+5$ is odd.

(2) ($\Rightarrow$) Suppose x is even. Then $x = 2k$ for some $k \in \mathbb{Z}$, so

$$3x+5 = 3 \cdot 2k+5 = 6k+5 = 2(3k+2)+1,$$

therefore $3x+5$ is odd.

Parts (1) and (2) combine to show that x is even iff $3x+5$ is odd.

(b) Equivalences of more than two statements / conditions.

("The following are equivalent ...")

Note: If $P \Rightarrow Q$ and $Q \Rightarrow R$ then $P \Rightarrow R$

So, to prove $(a) \Leftrightarrow (b) \Leftrightarrow (c)$ it suffices to show
$$\begin{tikzcd} (a) \arrow[rr, Rightarrow] & & (b) \arrow[dl, Rightarrow] \\ & (c) \arrow[ul, Rightarrow] & \end{tikzcd}$$,

(4 implications) (3 implications)

and to prove (a), (b), (c), (d) are equiv it suffices to show
$$\begin{tikzcd} (a) \arrow[r, Rightarrow] & (b) \arrow[r, Rightarrow] & (c) \arrow[r, Rightarrow] & (d) \arrow[lll, Rightarrow, bend left] \end{tikzcd}$$.

Ex. Let $n \in \mathbb{Z}$. Prove that the following conditions are equivalent.

(a) n is odd.

(b) $n^2 \equiv 1 \pmod 4$.

(c) n^2 is odd.

Pf: (a) $\Rightarrow$ (b) : Suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$, so

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv 0 + 0 + 1 = 1 \pmod 4.$$

(b) $\Rightarrow$ (c) : Suppose $n^2 \equiv 1 \pmod 4$, then $n^2 = 4k+1$ for some $k \in \mathbb{Z}$.

We can write $n^2 = 2(2k)+1$, so n^2 is odd.

(c) $\Rightarrow$ (a) : We need to show that n is odd if n^2 is odd, which we have proven before and will omit here.

By the above, we have that (a), (b), (c) are equivalent.

2. Existence proofs

Easier 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 $1729 = 10^3 + 9^3 = 1^3 + 12^3$, which suffices as an example.

(one can find this example by some computer program)

Point: · Construction and verification of an example is sufficient for proving an existential statement.

A harder example:

Prop: If $a, b \in \mathbb{N}$, then $\exists\, k, l \in \mathbb{Z}$ s.t. $\gcd(a,b) = ak + bl$.

(E.g. $a = 10$, $b = 12$ $\Rightarrow$ $\gcd(a,b) = 2$, $\quad -7 \cdot 10 + 6 \cdot 12 = 2$.

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

Pf: Consider the set $D = \{ax + by : x, y \in \mathbb{Z}\}$, and let d be the smallest positive integer in D. We claim that $d = \gcd(a,b)$, so that $\gcd = d = ak + bl$ for some $k, l \in \mathbb{Z}$ and we are 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 $r \in \{0, \dots, d-1\}$ be the remainder obtained when we divide a by d, so that $a = dq + r$ for some $q \in \mathbb{Z}$. We have

$r = a - dq$. But $d \in D$, so $d = ax + by$ for some $x, y \in \mathbb{Z}$, hence

$$r = a - dq = a - (ax + by)q = a(1 - xq) + b(yq) \in D.$$

Since d is the smallest positive number in D and $r \in \{0, 1, 2, \dots, d-1\}$,

it follows that $r = 0$. so $d \mid a$. A similar argument shows $d \mid b$.

We'll finish the proof (and do more proofs) next time.