Ch. 7 Proving Non-Conditional Statements

If & only if
Equivalent statements
Existence, existence & uniqueness
Constructive vs. non constructive proofs

§7.1 If and only if

To prove $P \iff Q$, we must prove both conditional statements

$P \Rightarrow Q$ and $Q \Rightarrow P$ (converse statements).

For each, we can use
(1) Direct proof,
(2) Contrapositive, or
(3) Proof by contradiction.

ex. **2.** Suppose $x \in \mathbb{Z}$. Then x is odd if and only if $3x+6$ is odd.

Proof:

First we show that if x is odd then $3x+6$ is odd.
We do this directly.
Assume $x = 2n+1$ for some $n \in \mathbb{Z}$.
Then $3x+6 = 3(2n+1)+6 = 6n+8+1 = 2(3n+4)+1$.
Since $3n+4 \in \mathbb{Z}$, it follows that $3x+6$ is odd.

Conversely, we now show that if $3x+6$ is odd then x is odd.
We do so by proving the contrapositive statement:
If x is even then $3x+6$ is even.
Assume $x = 2n$ for some $n \in \mathbb{Z}$.
Then $3x+6 = 3(2n)+6 = 2(3n+3)$.
Since $3n+3 \in \mathbb{Z}$, it follows that $3x+6$ is even.
This completes the proof. ∎

§7.2 Equivalent Statements

The following are equivalent:
(1) $P(x)$
(2) $Q(x)$
(3) $R(x)$
(4) $S(x)$

means $\big(P(x) \iff Q(x)\big) \wedge \big(Q(x) \iff R(x)\big) \wedge \big(R(x) \iff S(x)\big)$

But instead of proving these 6 conditional statements,
we have options.

$$\begin{array}{ccc} P(x) & \Rightarrow & Q(x) \\ \Uparrow & & \Downarrow \\ S(x) & \Leftarrow & R(x) \end{array}$$

4 conditional statements

If $P(x)$ is true then $Q(x)$ & if $Q(x)$ is true ...

If $P(x)$ is false then $S(x)$ is false
& if $S(x)$ is false ...

OR

$$\begin{tikzcd}[column sep=small] P(x) \arrow[r, Rightarrow] & Q(x) \arrow[r, Leftrightarrow] \arrow[dl, Rightarrow] & S(x) \\ R(x) \arrow[u, Rightarrow] & & \end{tikzcd}$$

(5 CONDITIONAL STATEMENTS)

OR ANY SET OF IMPLICATIONS SO THAT IF ANY STATEMENT IS TRUE THEN ALL STATEMENTS ARE TRUE, AND IF ANY STATEMENT IS FALSE THEN ALL STATEMENTS ARE FALSE.

NOTE: MORE EQUIVALENT STATEMENTS → MORE WAYS TO PROVE IT.
e.g. 6 STATEMENTS (a)-(f):

$$\begin{array}{ccccc} (a) & \Longrightarrow & (b) & \Longrightarrow & (c) \\ \Uparrow & & & & \Downarrow \\ (f) & \Longleftarrow & (e) & \Longleftarrow & (d) \end{array}$$

6 CONDITIONAL STATEMENTS

$$\begin{array}{ccccc} (a) & \Longrightarrow & (b) & \Longleftrightarrow & (c) \\ \Uparrow & & \Downarrow & & \\ (f) & \Longleftarrow & (e) & \Longleftrightarrow & (d) \end{array}$$

7 CONDITIONAL STATEMENTS

$$\begin{array}{ccccc} (a) & \Longleftrightarrow & (b) & \Longleftrightarrow & (c) \\ & & \Updownarrow & & \\ (f) & \Longleftrightarrow & (e) & \Longleftrightarrow & (d) \end{array}$$

CONDITIONAL STATEMENTS

§7.3 EXISTENCE PROOFS, EXISTENCE & UNIQUENESS PROOFS

ex.

Proposition There exists an even prime number.

Proof. Observe that 2 is an even prime number. ■

EXISTENCE THM: THERE EXISTS A FUNCTION f SUCH THAT f IS DIFFERENTIABLE AT 0 BUT f' IS NOT CONTINUOUS AT 0.

PROOF: CONSIDER $f(x) = \begin{cases} x^2 \sin\left(\frac{1}{x}\right) & \text{IF } x \neq 0 \\ 0 & \text{IF } x = 0 \end{cases}$.

THEN $f'(0) = \lim\limits_{x \to 0} \dfrac{f(x) - f(0)}{x - 0} = \lim\limits_{x \to 0} \dfrac{x^2 \sin\left(\frac{1}{x}\right)}{x} = \lim\limits_{x \to 0} x \sin\left(\frac{1}{x}\right)$

SINCE $-x \leq x \sin\left(\frac{1}{x}\right) \leq x$ FOR ALL $x \neq 0$, IT FOLLOWS (BY THE SQUEEZE THEOREM) THAT

$$f'(0) = \lim_{x \to 0} x \sin\left(\frac{1}{x}\right) = 0.$$

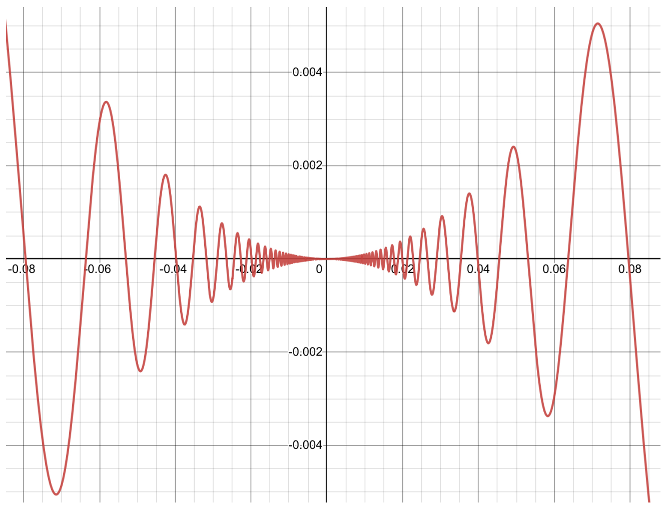
IN PARTICULAR, f IS DIFFERENTIABLE AT 0.

Now $f'(x) = \begin{cases} 2x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$.

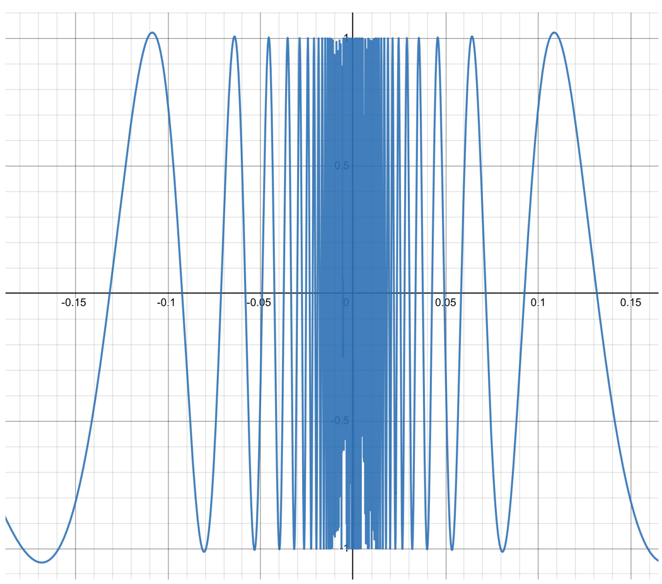
But $\lim\limits_{x \to 0} f'(x) = \lim\limits_{x \to 0} 2x \sin\left(\frac{1}{x}\right) - \cos\left(\frac{1}{x}\right)$

$$= \underbrace{\lim_{x \to 0} 2x \sin\left(\frac{1}{x}\right)}_{0} - \underbrace{\lim_{x \to 0} \cos\left(\frac{1}{x}\right)}_{\text{does not exist.}} \quad \text{does not exist.}$$

Thus $\lim\limits_{x \to 0} f'(x) \neq f'(0)$, i.e. f' is not continuous at 0. ■



$y = f(x)$



$y = f'(x)$

Proposition 7.1 If $a,b \in \mathbb{N}$, then there exist integers k and ℓ for which $\gcd(a,b) = ak + b\ell$.

e.g. $\text{GCD}(12,16) = 4 = (3)(12) + (-4)(16)$
$\text{GCD}(14,22) = 2 = (-3)(14) + (2)(22)$

PROOF: ASSUME $a, b \in \mathbb{N}$.
CONSIDER THE SET $A = \{ax + by : x, y \in \mathbb{Z}\}$. A CONTAINS BOTH POS & NEG ELEMENTS.

SET d = SMALLEST POSITIVE ELEMENT OF A, WITH $d = ak + b\ell$ FOR SOME $k, \ell \in \mathbb{Z}$.

WE NOW SHOW THAT $d = \text{GCD}(a,b)$ BY SHOWING $d \mid a$, $d \mid b$ (SO d IS A COMMON DIVISOR OF a & b), AND d IS THE GREATEST COMMON DIVISOR OF a & b.

THE DIVISION ALGORITHM GIVES $a = dq + r$ FOR SOME $q, r \in \mathbb{Z}$ WITH $0 \leq r < d$.
THAT IS,
$$r = a - dq = a - (ak + b\ell)q = a(1 - kq) + b(-\ell q).$$

THUS $r \in A$. SINCE d IS THE SMALLEST POSITIVE ELEMENT OF A AND $0 \leq r < d$, IT FOLLOWS THAT $r = 0$. THUS $d \mid a$.

A SIMILAR ARGUMENT WITH $b = dq + r$ WITH $0 \leq r < d$ SHOWS $d \mid b$.

THUS d IS A COMMON DIVISOR OF a & b.

LET $a = \text{GCD}(a,b) \cdot m$ AND $b = \text{GCD}(a,b) \cdot n$ FOR SOME $m, n \in \mathbb{Z}$.
SO $d = ak + b\ell = \text{GCD}(a,b) \cdot mk + \text{GCD}(a,b) \cdot n\ell$
$= \text{GCD}(a,b)(mk + n\ell)$.
THUS d IS A (POSITIVE) MULTIPLE OF $\text{GCD}(a,b)$ AND SO $d \geq \text{GCD}(a,b)$.
SINCE d IS A COMMON DIVISOR OF a, b, IT CANNOT BE GREATER THAN $\text{GCD}(a,b)$.

THEREFORE, $d = \text{GCD}(a,b)$. ∎

Example 2.5.3 (The universe is $\mathbb{R}$.) *There is a unique function* $f(x)$ *such that* $f'(x) = 2x$ *and* $f(0) = 3$.

Proof. *Existence*: $f(x) = x^2 + 3$ works.

Uniqueness: If $f_0(x)$ and $f_1(x)$ both satisfy these conditions, then $f_0'(x) = 2x = f_1'(x)$, so they differ by a constant, i.e., there is a C such that $f_0(x) = f_1(x) + C$. Hence, $3 = f_0(0) = f_1(0) + C = 3 + C$. This gives $C = 0$ and so $f_0(x) = f_1(x)$. ∎

§7.4 Constructive vs. Non-Constructive Proofs

Proposition There exist irrational numbers x, y for which x^y is rational.

We show such things exist without explicitly saying what they are

$\downarrow$

Proof: (Non-constructive). Let $a = \sqrt{2}^{\sqrt{2}}$ & $b = \sqrt{2}$.

If a is rational, then set $x = \sqrt{2}$, $y = \sqrt{2}$.
That is, x & y are irrational and x^y is rational.

If a is irrational, then set $x = a = \sqrt{2}^{\sqrt{2}}$ & $y = b = \sqrt{2}$.

Then x & y are irrational and $x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$ is rational.

We give an explicit example.

$\downarrow$

Proof: (Constructive). Let $x = \sqrt{2}$ & $y = \log_2 9$.

Then $x^y = \sqrt{2}^{\log_2 9} = \sqrt{2}^{\log_2(3^2)} = \sqrt{2}^{2\log_2 3} = 2^{\log_2 3} = 3$ is rational.

Since $\sqrt{2}$ is irrational (previously proved in Ch. 6), we are done if we can show $\log_2 9$ is irrational.

Assume, by way of contradiction, $\log_2 9 = \frac{a}{b}$, $a, b \in \mathbb{Z}$.

Then $2^{a/b} = 9$, i.e. $2^a = 9^b$.

But 2^a is even & 9^b is odd $\Rightarrow\Leftarrow$. ■